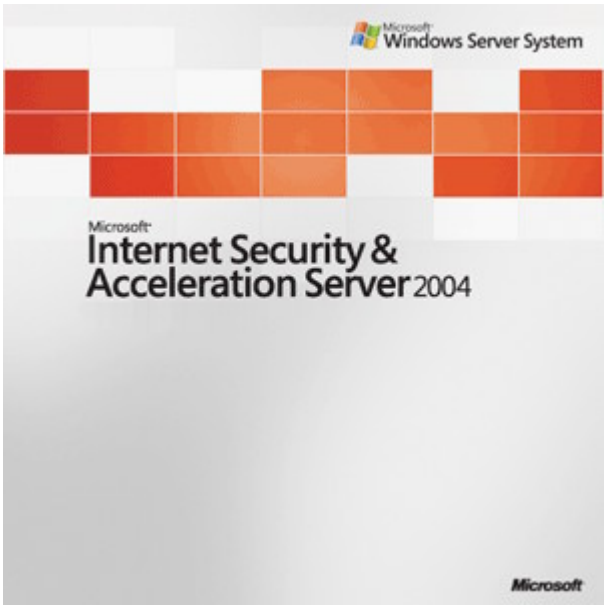
منهاج آيزا سيرفر 2004



المنهاج مقدم من شبكة الجيل الجديد للتكنولوجيا
www.itnat.com

- من إعداد: م. فادي بطة fmfm
- متابعة: م. رامي ربايعة NaT-Server

26 كانون الثاني 2007

إهـــــداء

نهدي هذا الكتاب الى كل طالب علم والى كل من يحتاجه، وهذه النسخة مجانية ولا نبغي منكم سوى الدعاء لنا وللقائمين على الموقع بالخير والهدى وأن يشفي آبائنا وأمهاتنا ويرحمنا دنيا وآخرة.

ملاحظة: يسمح بنقل الكتاب ونشره.

الفهرس:

تم افتتاح دورة الايزا 2004

السلام عليكم ورحمة الله وبركاته

الحقيقة نشكر الأعضاء وزوار الموقع والنشيطين منهم بالذات، بالسماح لنا بتقديم مالم يقدم على الشبكة العنكبوتية وباللغة العربية ،، من خلال خبرتنا ومعرفتنا بسوق العمل نعلم ماهو المطلوب تحديداً للتميز والظهور بأفضل نتائج ، ومن خلال شبكة الجيل الجديد للتكنولوجيا فقد قمنا بفتح قسم جديد للدورات وهانحن الان نقدم الدورة الثانية بجانب دورة بناء سيرفر مثالي2005 ، وهي دورة آيزا سيرفر 2004 ،، من خلال هذه الدورة ستتعلم كيفية اعداد الآيزا سيرفر وبطريقة محترفة فعلاً وهي مقسمة على عشرة دروس دسمة نراها بعد قليل في الخطة الدراسية للدورة.

دورة ايزا سيرفر
2004
اهلا بكم جميعا في دورة الايزا 2004

مقدمة:

بالنسبه للاعمال والشركات اصبحت الشبكات عنصر اساسي لا يتجزأ من بنيتها التحتيه حتى تتمكن من اداء مهامها على اكمل وجه في عصر التكنولوجيا، وكما تعرفون فان قلب الشبكه هو السيرفر
- لمعرفة المزيد عن السيرفر راجع هذا الرابط:
http://www.itnat.com/forum/showthrea...newpost&t=3270

لكن ماذا عن الامن والتحكم، صحيح ان ويندوز سيرفر يقدم لك الكثير من الادوات لادارة الشبكه لكن يبقى عنصر الامان عنصر مهم ولا يستطيع الويندوز سيرفر الاهتمام به لوحده، لذلك قامت مايكروسوفت بطرح الايزا سيرفر (Microsoft Internet Security and Acceleration Server) وهو سيرفر الامن والسرعه

بالعربي وبطريقة أخرى هو سيرفر يهتم بتوزيع الإنترنت على المستخدمين ، ومن مزاياه الرائعة بانه يتناسب مع ويندوز 2003 سيرفر بطريقة سلسة مما يقدم لدينا أقوى سيرفر على نسخ ويندوز على الإطلاق.

ما هو الآيزا سيرفر:

الآيزا سيرفر هو جيل جديد متتابع من منتجات مايكروسوفت ، وقد بدأ بنسخة Proxy server قبل العام 2000 وصدرت بعد العام 2000 النسخ التالية على التوالي :آيزا 2000 وآيزا 2004 وآيزا 2006 ،، وأفضلها وأقواها الآن هي نسخة آيزا2004 ، هذا السيرفر العجيب الذي يسمح لك بتوزيع الانترنت تحت صلاحيات عالية ، وتتحكم بموارد الشبكة التي تختص بتوزيع الانترنت بأكثر من طريقة ،، ويمتاز هذا السيرفر بوجود نظام الكاش الخاص به Cash Server الذي يزيد من سرعة الانترنت وكذلك له منتجات تدعمه من شركات أخرى سنتطرق لها بعد الانتهاء من الدورة.

في هذه الدورة سوف نقوم بشرح اهم مميزات وخصائص الايزا وكيفية تنصيبه والتعامل معه حتى تتمكن من حماية شبكة الإنترنت الخاصة بك بشكل كامل ان شاء الله ، وسنتوسع بالموضوع بطريقة سلسة بحيث تفهم أكثر من مجرد تحميل الآيزا سيرفر.

الخطة الدراسية للدورة:

-مقدمة للايزا ومميزاته
-طريقة تنصيب خدمات الشهادات Certificate Services
-تنصيب خدمه DHCP و DNS ودعمها لـ الفايرول والويب بروكسي Firewall & Web Proxy بحيث يتناسبان مع الايزا من غير تحميل الآيزا كلينت
-تنصيب الآيزا سيرفر 2004 على ويندوز 2003 سيرفر
-طريقة عمل باك اب واسترجاع اعدادات الآيزا بصورة صحيحة.
-اعداد سياسات الوصول للايزا.Access Policy
-اعدادات الإكسشينج سيرفر من خلال الآيزا.
-تفعيل خدمة الكاشCaching
-السماح لإتصالات الـ VPN من خلال الآيزا سيرفر

نقاط مهمة:

1.سيتم وضع كل درس أسبوعياً، وبنفس سياسة الدورات الأخرى.
2.يوجد فترة أسبوع لمن لديه أسئلة في مجال الدرس.
3.سيتم الإجابة على الأسئلة قبل وضع الدرس الثاني وستضاف في الدرس كأسئلة شائعة وتحفظ بملف للتحميل.
4.لن يتم الإجابة على أسئلة أخرى في الدرس بعد اضافة الدرس الذي بعده وسيتم اقفال الردود للحفاظ على مسيرة الدورات.
5.يسمح بنقل الموضوع بغرض الفائدة الى مواقع أخرى مع ذكر المصدر.
6.يسمح بالمداخلات وسيتم اعتمادها بالدرس الأصلي باسم كاتب المداخلة.

ولمن لديه استفسار أو سؤال يتفضل ليضعه هنا

مقدم الدورة: فادي بطه(fmfm)

الدرس الأول
مقدمة للايزا ومميزاته

أهلا بكم في دورة الايزا 2004، هذه الدورة معده لمساعدتك على البدء في استخدام الايزا لحماية شبكتك والسماح باتصال امن اليها. الجدران الناريه عادة تكون من اصعب اجزاء الشبكه من ناحية الاعداد، حيث يلزم معرفة في مبادئ الشبكات و بروتوكولات TCP/IP حتى تفهم كيفيه عملها، لكن مع الايزا لا داعي لكل هذا حيث انه منتج يوفر لك سهوله وفعاليه في تنصيب الجدار الناري والتحكم بالشبكه.
بشكل عام يمكن ان نقول ان مبدا الايزا ببساطه كالتالي: اذا كان هناك اتصال يسمح بتبادل المعلومات عن طريق الجدار الناري فان الايزا يسمح له بالاتصال اما غير ذلك فيتم قطع الاتصال.
ايضا الجدران الناريه لا تعمل لوحدها حيث يجب وجود خدمات اخرى تساعد الجدار الناري على اداء مهمته وسوف نتحدث عن هذه الخدمات من ضمن الدورة.
وقبل ان نبدأ يجب ان نذكر ملاحظه مهمه وهو ان تكون الشبكه معدة بشكل جيد وجاهزة لتنصيب الايزا حتى تتلافى الاخطاء الشائعه التي تحصل بسبب عدم اعداد الشبكه بشكل جيد.

ما هو الايزا سيرفر

حسب تعريف مايكروسوفت للايزا فهو عباره عن integrated security edge gateway يعني بعباره اخرى حارس للشبكه ومراقب للداخل والخارج منها

ما الجديد فيه عن الايزا2000

يمكن تلخيص مزايا الايزا الجديد حسب الفئات التاليه

الفلتره على مستوى التطبيقات:

-فلترة عناوينhttp
-منع الوصول الى الملفات التنفيذيهexe
-تحديد الملفات المسموح تحميلها
-التحكم في الوصول الى مواقع http حسب توقيع الموقع
-التحكم في البيانات المرسله عن طريق http ، مثلا يمكنك منع المستخدمين من ارسال معلومات عن طريق امر postالخاص ب.http
-التحكم ببروتوكول ftp مثل السماح فقط بالتنزيل او التحميل.
-مترجم الروابط، وهي خاصيه متقدمه الهدف منها هو ترجمة المواقع الموجوده على الشبكه المحليه الى عناوين يمكن الوصول اليها من الانترنت، لان المستخدم الخارجي يصل فقط الى الايزا والحائط الناري.

الحمايه والحائط الناري:

-تحكم متقدم بالبروتوكولات مثل بروتوكولip
-دعم للبروتوكلات المعقده التي تتطلب اكثر من وصله مثل اتصالات الفيديو
-عمل مجموعات حائط ناري حيث يمكنك تحديد اعدادات خاصه لكل مجموعه
-التحقق من الهويه باستخدام ال RADUIS الخاص بالويندوز
-الوصول الى بريد هوتميل من خلال الحائط الناري

سهولة الاستخدام:

-تنصيب اكثر من شبكه
-عمل بوليسي خاصه بكل شبكه
-نماذج شبكات جاهزة

المراقبه والتقرير:

-مراقبه لمدخلات اللوجات بشكل مباشر
-مراقبه وفلترة جلسات الفايرول بشكل مباشر
-التحقق من الوصلات
-ارسال بريدي الكتروني بالتقرير

الادارة:
-استيراد وتصدير الاعدادات
-منح صلاحيات للمستخدمين
-تحكم في الدخول للمستخدمين
-بوليسي للشركات
والكثير من المميزات الاخرى مثل مميزات الشبكات الخاصه vpn وميزه مهمه في الايزا وهي الكاش caching حيث يقوم بتخزين المواقع التي تم الوصول اليها حتى اذا طلبت مره اخرى يتم توفيرها بشكل اسرع والتخفيف على الخط الرئيسي للانترنت.
عند تنصيب الايزا لا يشترط استخدام كل المميزات وهذا ما يميزه حيث بامكانك ان تطوع الايزا حسب شبكتك ومتطلباتك، بعض الشبكات تتطلب منع المسنجر وشبكات اخرى تسمح وهكذا.
هكذا نكون انهينا المقدمه عن الايزا ومميزات بانتظار استفساراتكم، في الدرس القادم سوف نتحدث عن طريقة تنصيب خدمات الشهادات Certificate Services واهميتها في استخدام البروتوكولات وتفعيل الشبكه الخاصه vpn .

الدرس الثاني
طريقة تنصيب خدمات الشهادات Certificate Services

مقدمة

لبناء شبكه قويه وامنه ستحتاج الى تنصيب الكثير من الخدمات، منها خدمة الشهادات Certificate Service هذه الخدمه تعتبر اساس SSL وهو نظام تبادل معلومات امني قوي يعمل على فحص الشهاده والتاكد من مصدرها ومحتواها للسماح بتبادل المعلومات المهمه، افضل مثال عليها شهادات موقع hotmail حيث تصادف كل فتره ان المتصفح يطلب منك الموافقه على الشهاده لان اتصالك يعتبر الى نطاق امني.

طريقة التنصيب

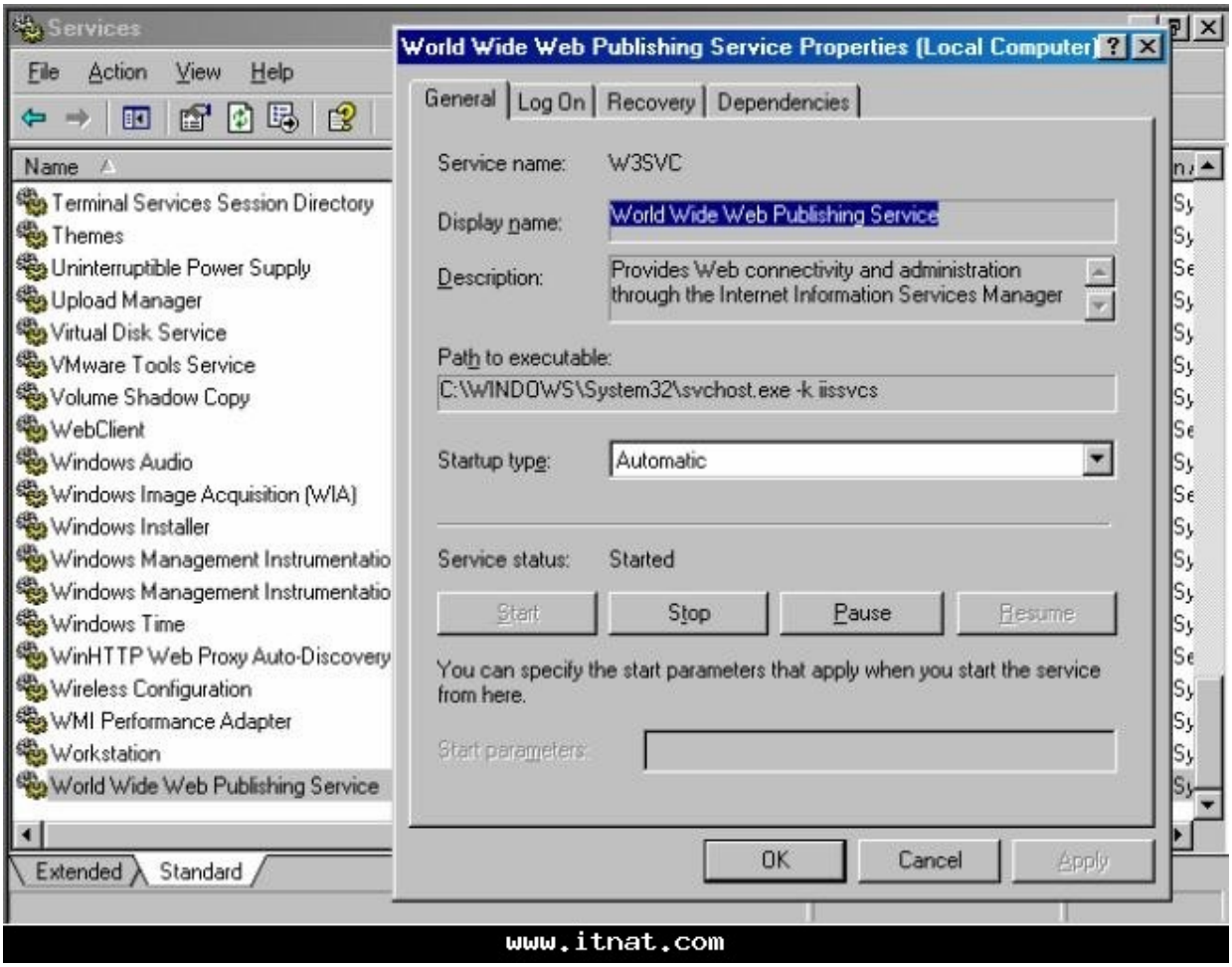
خدمة الشهادات من مايكروسوفت يمكن ان تنصب على الدومين على الشبكه الداخليه لتصدر شهادات للاجهزة على الشبكه الداخليه وكذلك الاجهزة التي ليست جزء من الشبكه، سوف نستخدم هذه الشهادات في دورتنا لتحقيق التالي:
-السماح للايزا سيرفر باستخدام بروتوكول L2TP/IPSec VPN لعمل اتصال vpn من موقع الى موقع.
-السماح للايزا سيرفر باستخدام بروتوكول L2TP/IPSec VPN لعمل اتصال بين عميل vpn
-السماح للمستخدمين باستخدام بروتوكول SSL للوصول الى مواقع الاوتلوك وتبادل البريد.
ال SSL (Secure Socket Layer) هو بروتوكول يقوم بتفير البيانات المنقوله بين جهاز العميل والسيرفر لضمان الامان وهو يعتبر الان افضل وسيله للحمايه على الانترنت بالاضافه الى ان الشهادات تساعد على التحقق من هويه الاجهزة التي تحاول الاتصال باستخدام بروتوكول vpn عن بعد.

تنصيب خدمه IIS 6.0

الهدف منها هو التاكد من خدمة النشر علىwww

- اضغط على ابدا ثم الى Administrative Tools ثم الخدمات Services
- اختار تاب standard من الاسفل وانزل الى خدمة World Wide Web Publishing Service وثم
- ين عليها لتفتح نافذه الخدمه
- لان تاكد من نوع البدايه للخدمه اوتوماتيكي وانها تعمل كما في الصورة

!

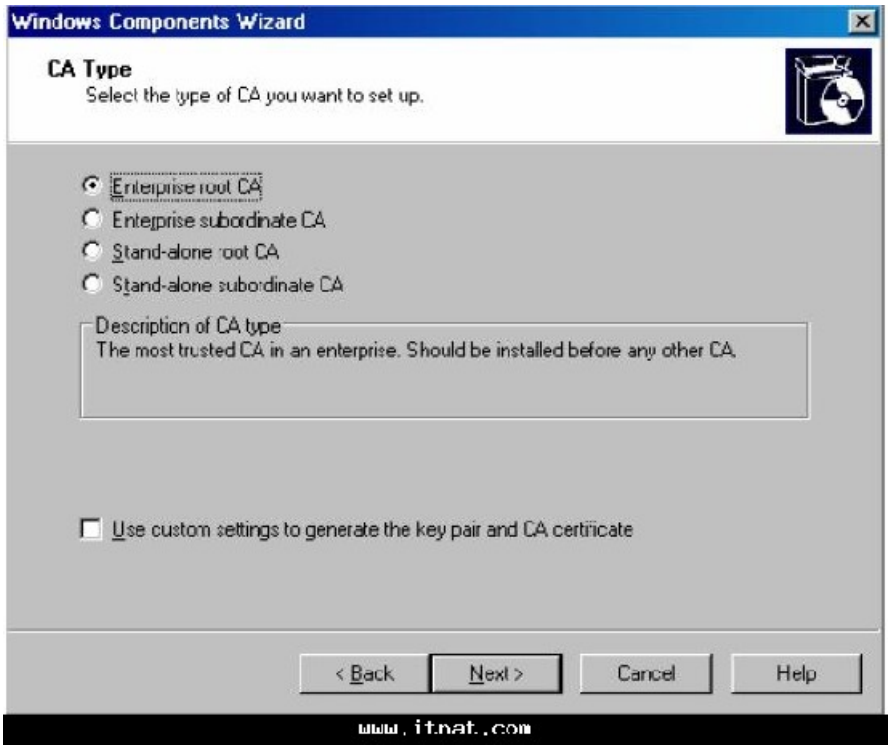


4-الان اغلق النافذه
5-هكذا تاكدنا ان خدمة النشر على الويب تعمل

الدرس الثالث:
تنصيب خدمة الشهادات من مايكروسوفت في بيئهCertificate Authority

خدمات الشهادات من مايكروسوفت تنصب في بيئة(Enterprise Certificate Authority)
ال CA هي عباره عن سلطه مركزيه في شبكه تقوم باصدار وادارة معطيات الامان في الشبكه للتراسل وتبادل المعلومات حيث تقوم بفحص الشهاده للجهه التي طلبت المعلومات، اذا كانت مطابقه لل Registration Authorityفان ال CA تصدر الشهاده.

طبعا يفصل تنصيب ال CA في بيئه Enterprise للاسباب التاليه:
1-الشهاده المركزيه تخزن اوتوماتيكيا في Trusted Root Certification Authorities حيث تخزن بدورها في جميع اجهزة الدومين.
2-يمكنك طلب شهادات موقع او جهاز بسهوله
3-يمكنك تخصيص شهادات للاجهزه والمستخدمين باستخدامActive Directory auto enrollment
طبعا يمكنك تنصيب CA في بيئه ستاندرد لكن لن يتم تغطيتها هنا لانها تحتاج الى اجراءات خاصه بالتنصيب وسحب الشهادات.
الان الخطوات لتنصيب Enterprise CA على جهاز المتحكم بالدومين
1-اضغط ابدا ثم لوحة التحكم
2-اضافه او الغاء البرامج ثم Add/remove windows components من اليسار
3-الان في صفحة المكونات ابحث عن Certificate Services وضع صح بجانبها سيظهر مربع حوار اضغط yesلتوافق انك لا تستطيع تغيير اسم الجهاز.
4-الان اضغط Next في صفحة Windows Components
5-في صفحه CA Type اختار خيار Enterprise root CA واضغطNext



6- في صفحة CA identifying Information سيطلب منك اسم ال CA في مربع Common Name for this CA، هنا تدخل اسم DNS Host لهذا المتحكم بالدومين وعادة يكون نفس اسم NetBIOS
7- اذا كنت نصبت هذه الخدمه سابقا سيظهر مربع لتاكيد الكتابه فوق الاعدادت السابقه، اذا كنت وزعت الشهادات على الاجهزة في الشبكه لا تقم باعادة الكتابه فوقه.
8- في صفحة Certificate Database Settings اختار المكان القياسي لقاعدة البيانات وسجل الشهادات واضغط التالي.
9- الان سيبلغك النظام ان خدمة IIS سيتم اعادة تشغيلها اضغط ليتم ذلك اوتوماتيكيا.
10- الان سيطلب منك قرص الويندوز ادخله ليسنخ الملفات المطلوبه
11- اضغط Finish

هكذا نكون نصبنا خدمة Enterprise CA ليقوم باصدار الشهادات اوتوماتيكيا عن طريق ال AD او Certificate mmc snap-in و. Web enrollment

---

الدرس الرابع
تنصيب خدمه DHCP و DNS ودعمها لـ الفايرول والويب بروكسي Firewall & Web Proxy بحيث يتناسبان مع الايزا من غير تحميل الآيزا كلينت

في هذا الدرس سنتعرف على بروتوكول(WPAD (Web Proxy Auto discovery Protocol

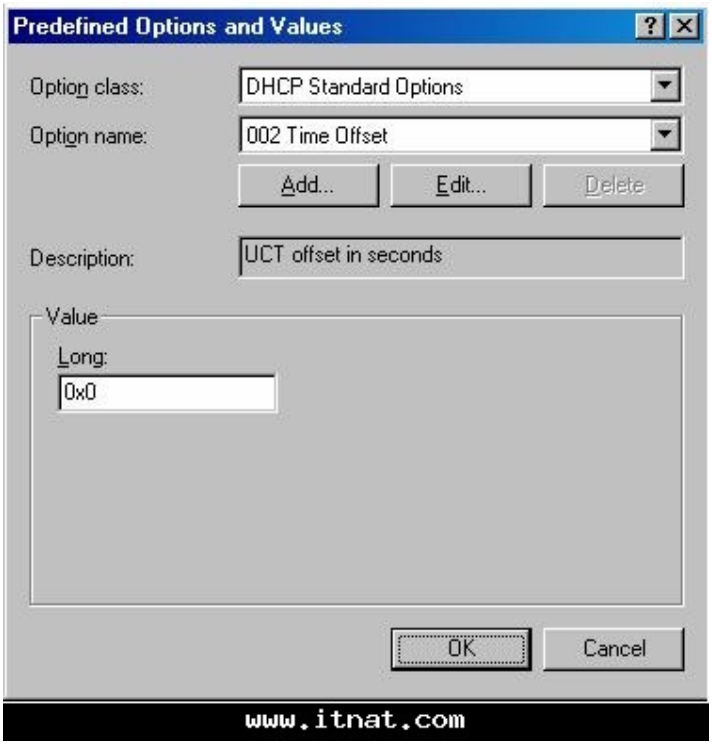
هذا البروتوكول يستخدم للسماح لمتصفحات الانترنت والفايرول على اجهزة المستخدمين من الوصول الى عنوان سيرفر الايزا 2004 بشكل اوتوماتيكي. حيث يقوم المستخدم بتحميل معلومات التنصيب الالي من الفايروول بعد ان يقوم البروكسي او الفايروول على جهاز المستخدم من التعرف عليه.

في هذا الدرس سنتعرف على كيفيه:
-اعداد DHCP WPAD و
-اعداد DNS WPAD
بعد ادخال معلومات ال wpad الى ال DNS DHCP فان المستخدمين لا يحتاجو الى تنصيب يدوي لتفعيل الاتصال بالانترنت عن طريق الايزا سيرفر 2004

اعداد WPAD علىDHCP

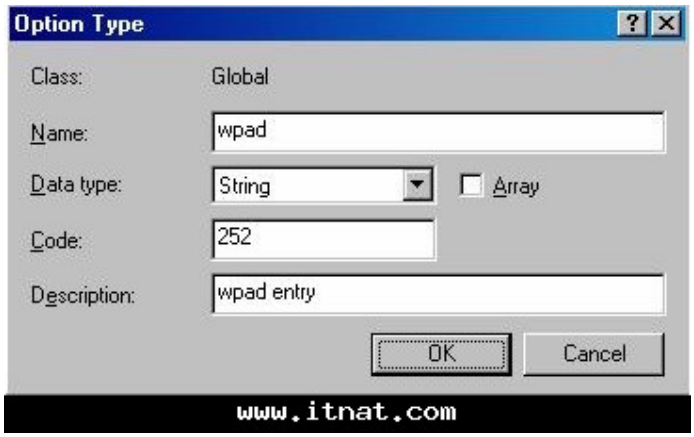
اول شيئ نقوم بعمل اعدادات لل DHCP خاصه بنا
1- افتح كونسول DHCP من Administrative Tools ثم اضغط على اسم السيرفر باليمين واختار Set Predefined Options.

2-اضغط اضافه فيPredefined Options and Values



3-سيظهر مربع حوار ادخل البيانات التاليه
Name: wpad
Data type: String
Code: 252
Description : wpad entry

اضغط اوكي

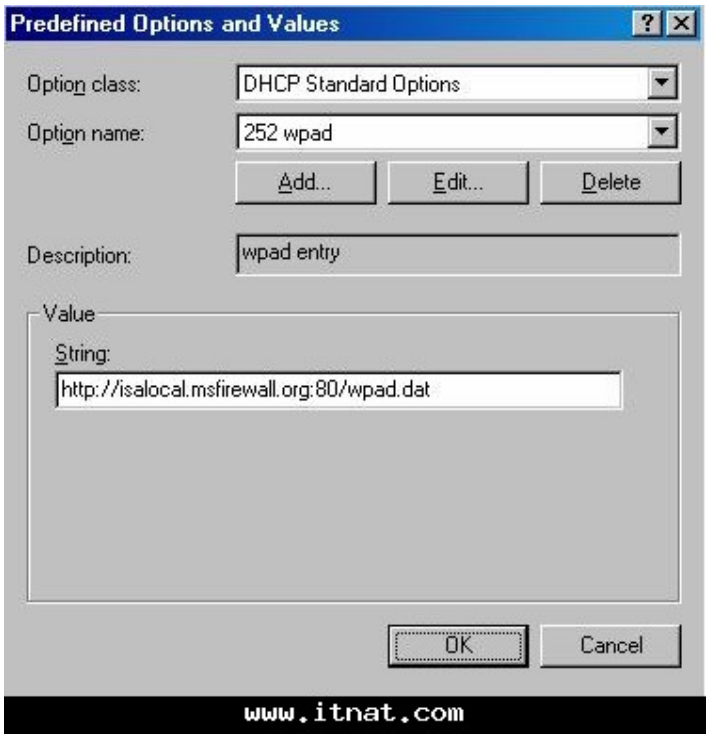


-4سيظهر اطار اسمه Value ، ادخل عنوان الفايروول في مربع string كالتالي

Server name:Atodiscovery port number/wpad.datهttp://Isa

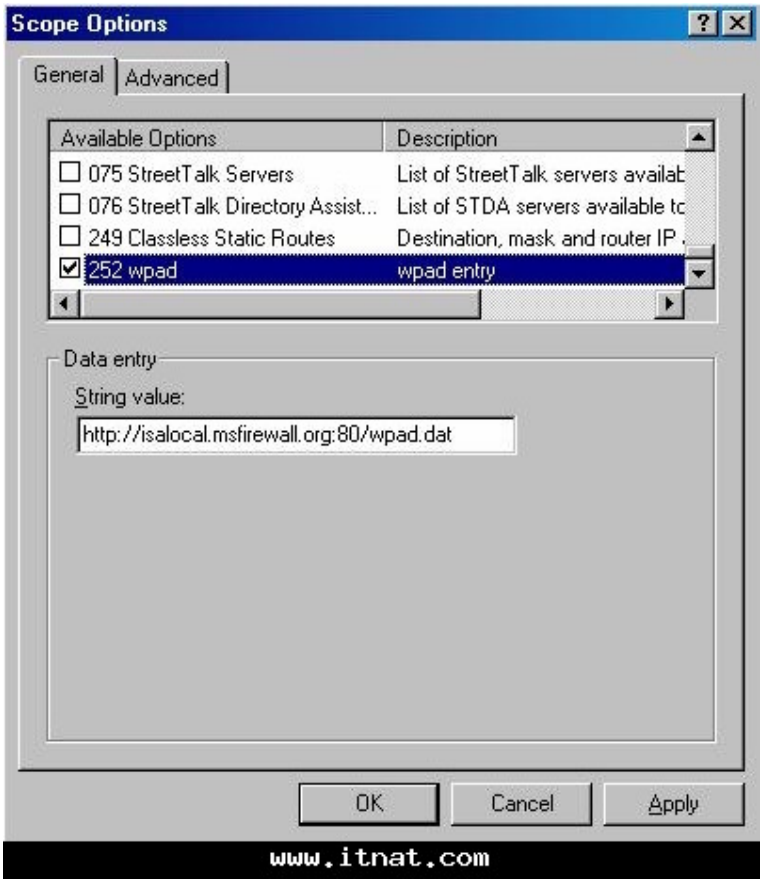
بدون المسافات طبعا، البورت يكون بالعاده 80 يمكنك تغيير هذه القيمه من كونسول التحكم بالايزا.
في مثالنا يكون العنوان كالتالي
http://isalocal.msfirewall.org:80/wpad.dat

لاحظ ان اسم ال wpad يجب يكون بالحروف الصغرى.Lower case
اضغط اوكي



-5 الان اضغط باليمين على Scope options واختار Configure options

-6 سيظهر مربع حوار فيه لائحه بالخيارات المتوفره انزل الى 252 wpad وضع صح عليه ثم تطبيق واوكي.



-7 الان ستظهر الكونسول الخاصه ب DHCP وفيها يظهر الخيار الذي قمنا باضافته تحت اسم wpad252

الان اغلق الكونسول، الان يستطيع اي مستخدم يملك صلاحيات ادمن على اي جهاز تابع لل DHCP يستطيع هذا الجهاز ان يستخدم ال wpadليقوم اوتوماتيكيا باكتشاف الفايرول التابع للايزا 2004 وبالتالي اعداد نفسه، لكن ايضا الفايرول نفسه يحتاج الى اعداد حتى يتمكن من دعم النشر التلقائي للاعدادات وهو ما سناتي على ذكره في هذا الدرس.

اعداد WPAD علىDNS

هذه طريقه اخرى لتوصيل المعلومات للمستخدمين على الشبكه عن طريق انشاء اسم wpad في DNS للسماح للمتصفح بالوصول الى معلومات الايزا واعداده على الجهاز. الفرق بين هذه الطريقه وبين طريقة ال DHCPهو ان هذه الطريقه لا يجب ان يكون المستخدم من مجموعة مستخدمين معينه حتى يقوم بتطبيق الاعدادات.

ملاحظه: عند استخدام طريقه نشر الفايرول والبروكسي على DNS فانه لا يمكن اختيار اي منفذ الا منفذ 80.

-انشاء ادخال wpad الىDNS

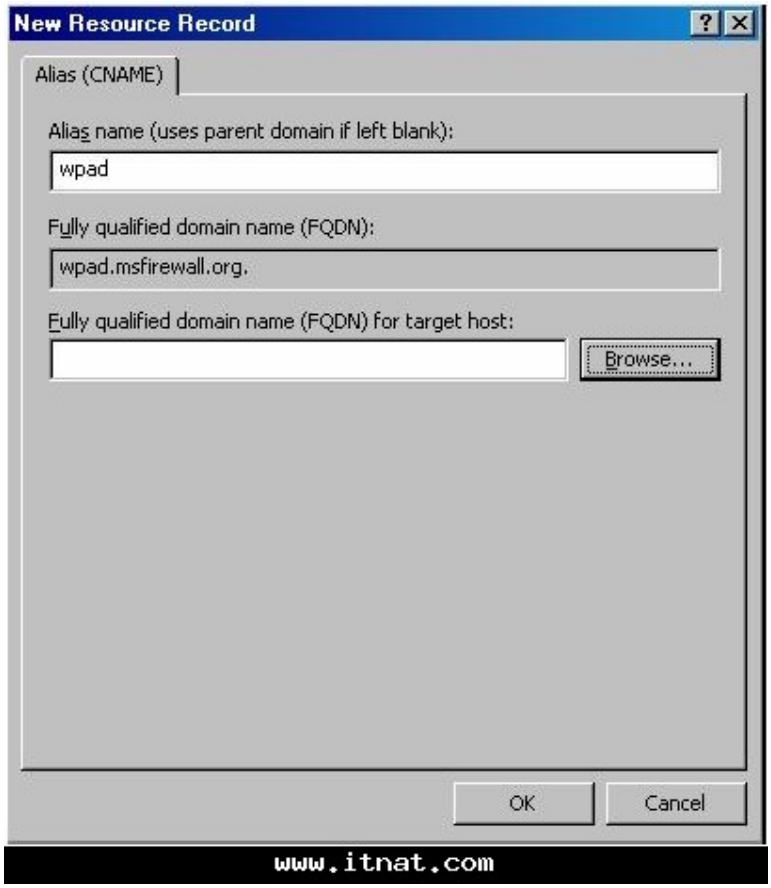
اول خطوة في تجهيز ال DNSهي انشاء اسم wpad فيه، هذا الاسم يدعى (alias) بالعربي يعني الاسم المرادف ويدعى ايضا (CNAME record) يقوم هذا الاسم المرادف بالاشارة الى سجل يدعي Host(A) حيث يقوم هذا السجل بتحويل اسم الفايروول الخاص بالايزا الى اي بي داخلي.

عند انشاء الاسم المرادف يجب اولا تجهيز سجل (A) لكن في حالتنا فان الايزا سيرفر قام بتسجيل نفسه اوتوماتيكيا (كعنصر اساسي في التنصيب) مع ال DNSوهكذا لا تحتاج لانشاء سجل ال (A)يدويا.

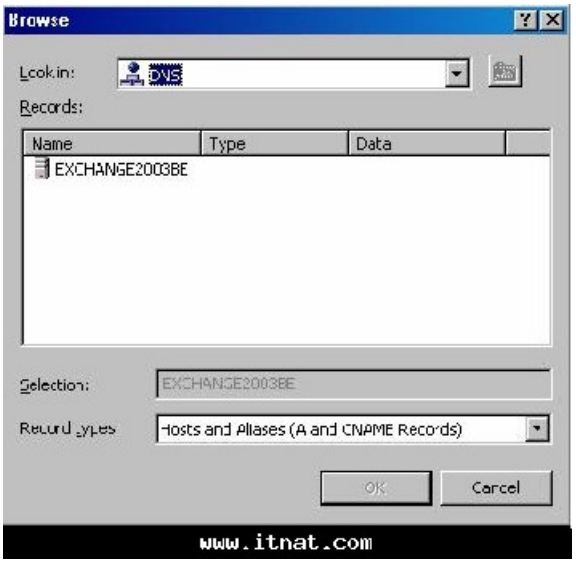
الان ننتقل الى الدومين لنقوم بتجهيز الاعدادت على الDNS

-1اذهب الى ابدأ ثم Administrative Tools اختار DNS ، الان ستظهر الكونسول الخاصه بادارة ال DNS ، سترى على اليسار مجلد اسمه Forward lookup zone اضغط عليه باليمين واختر New Alias (CNAME).

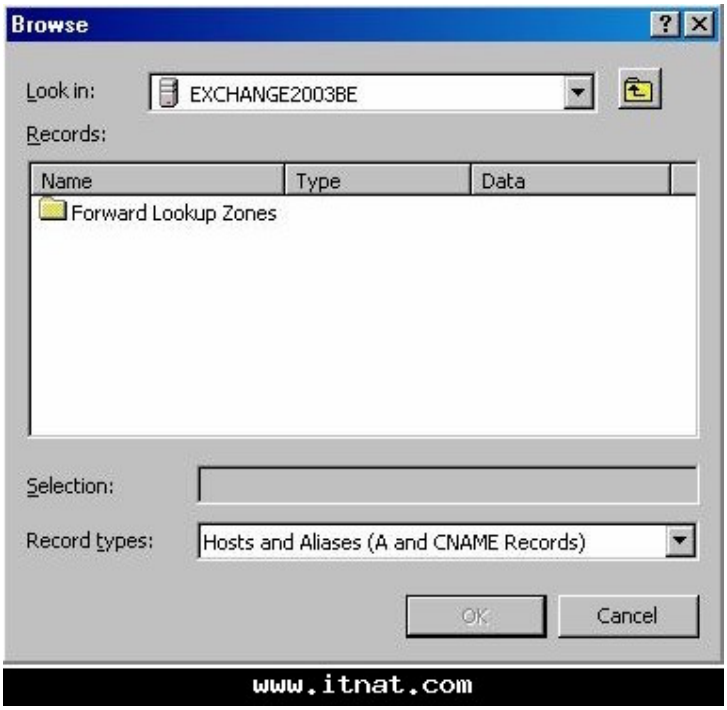
-2سيظهر مربع حوار ادخل الاسم المرادف wpad ثم اضغط علىbrowse



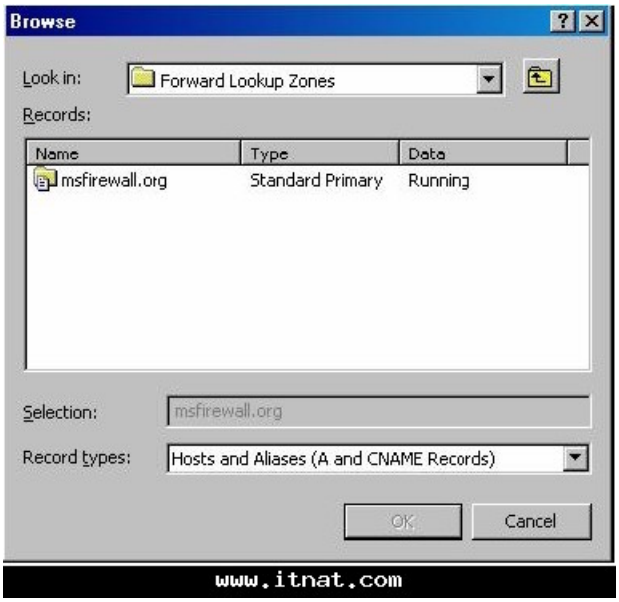
-3سيظهر سجلات، اضغط على اسم سيرفرك



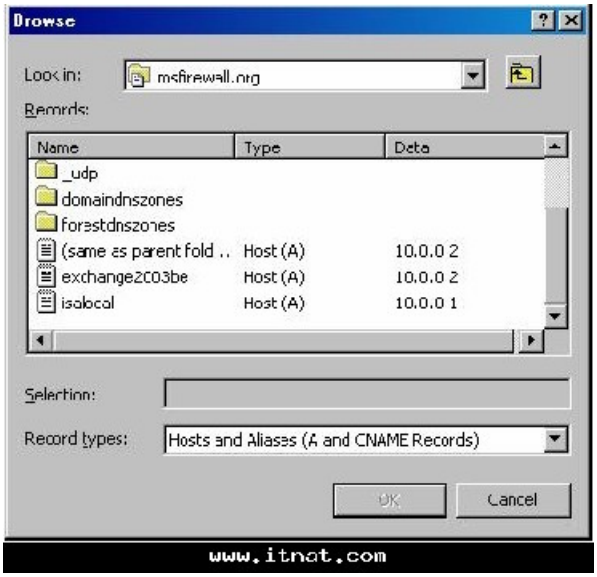
-4في مربع الحوار اضغط مرتين على Forward Lookup Zone في اطار السجلات.



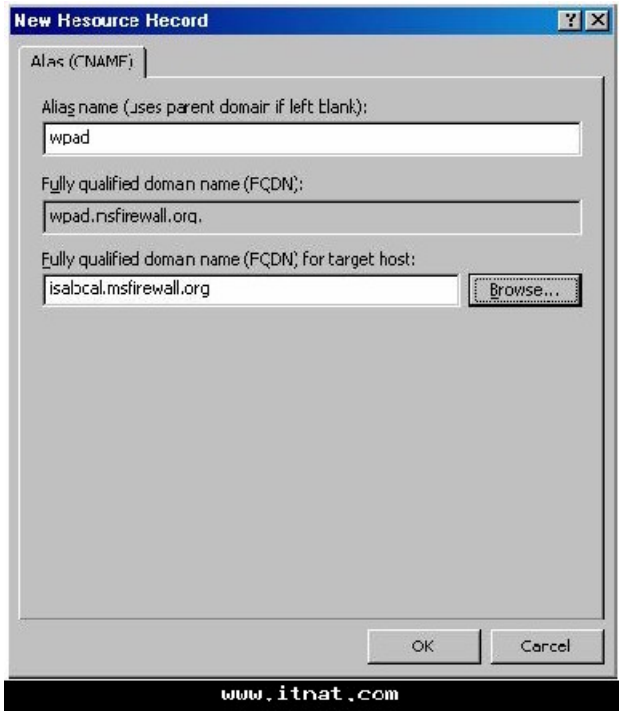
-5في النافذه التاليه اختار اسم فايروول الايزا

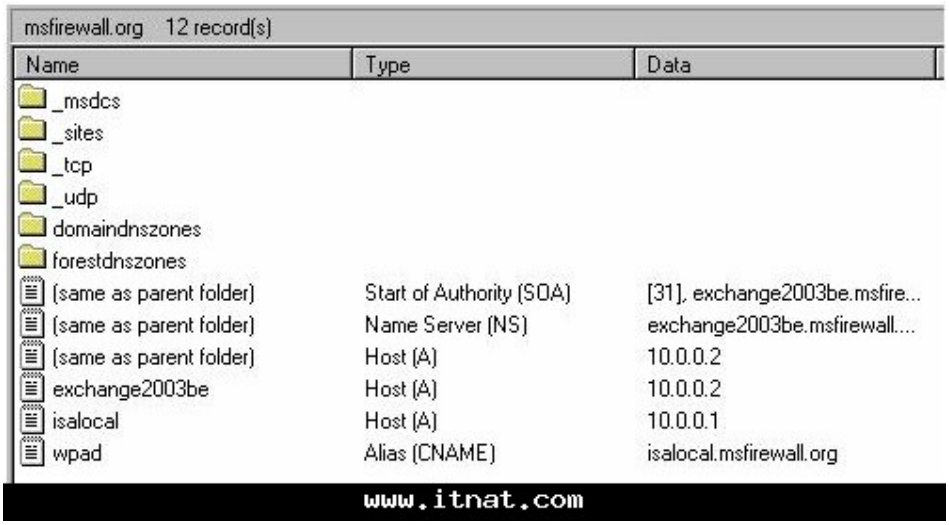


-6سيظهر مربع New Resource Record اضغطOK



-7ستظهر ادخاليه الاسم الجديد (CNAME) في الجزء الايمن من كونسول الDNS





-8اغلق الكونسول وهكذا نكون انتهينا من هذه الخطوه

الان ننتقل الى اعداد المستخدم للاستفاده من اسمWPAD

اولا يجب ان تعرف النقاط التاليه

-البروكسي(متصفح الانترنت) والفايروول الخاص بالمستخدم يجب ان يكون قادر على معرفه الاسمwpad
-البروكسي والفايروول لا يعرف اي دومين يحتوي اسم الwpad
-نظام التشغيل الخاص بالمستخدم يجب ان يكون قادرا على تزويد البروكسي والفايروول بهذه المعلومات

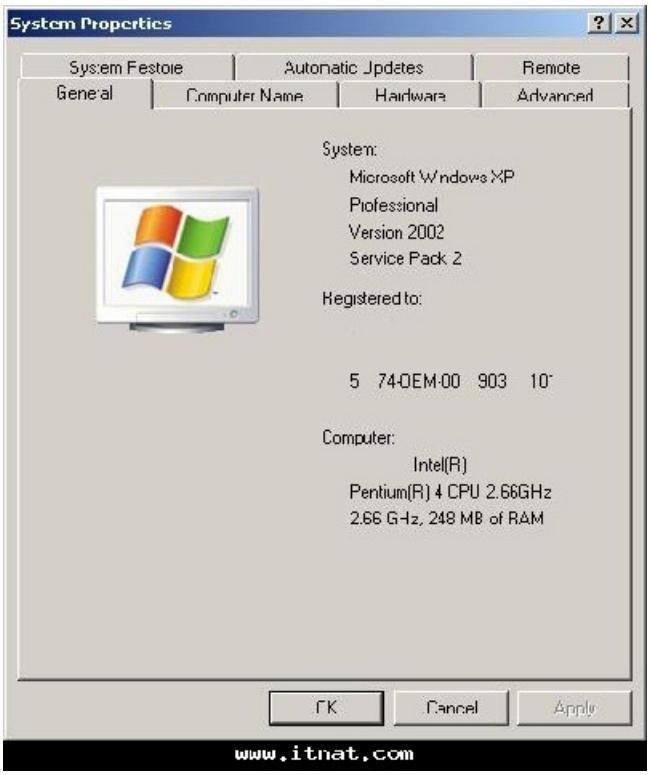
طلبات ال DNSيجب ان تكون مؤهله بالكامل قبل ارسالها الى سيرفر الDNS ، هذا يعني انها يجب ان تحتوي اسم المستخدم واسم الدومين(Host Name and Domain Name) ، كما ذكرنا قبل قليل فان البروكسي والفايروول يملكون فقط اسم المستخدم ، هنا يقوم نظام التشغيل الخاص بالمستخدم باضافه جزء اسم الدومين قبل ارسال الطلب الى سيرفر ال.DNS

هناك طريقتين للتاكد من ان اسم الدومين تم اضافته الى طلب ال wpad المرسل الى سيرفر الDNS

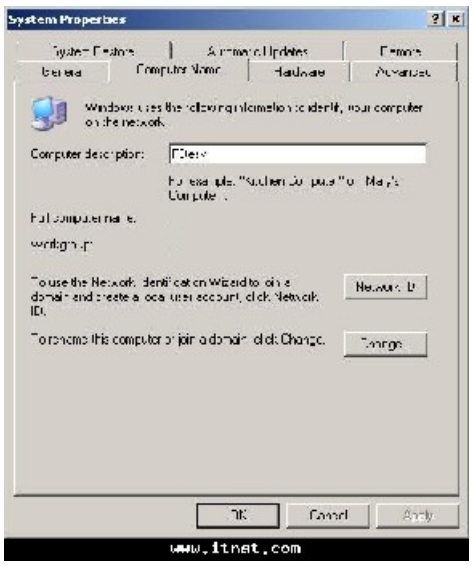
-استخدام DHCP لتعيين اسم دومين اساسي
-اعداد اسم الدومين على جهاز المستخدم في قسم تعريف الشبكه المحليه.

طبعا في حالة ان المستخدم جزء من الدومين ومدخل في Active Directory فسيكون ادخال اسم الدومين تلقائي، لكن اذا لم يكن المستخدم جزء من ال (Active Directoryوهي حالات قليله) عليك بالخطوات التاليه (على ويندوز اكس بي:(

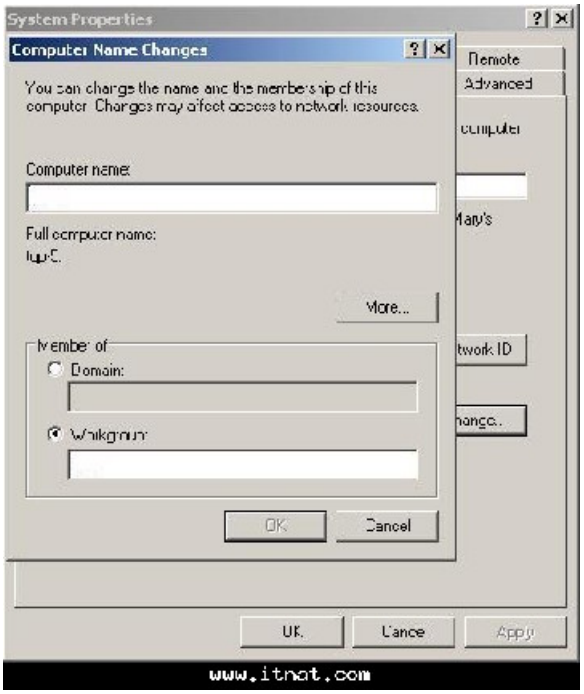
1-اختار خصائصMy Computer



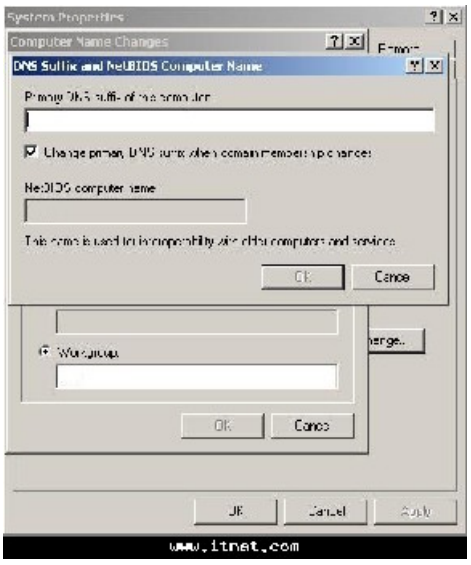
2-اضغط على لسان اسم الجهاز ثم اضغط علىChange



3-الان اضغط على More ليظهر مربع حوار



4-الان ادخل اسم الدومين في المربع الاول حتى يتم ادخاله في كل طلب الى ال.DNS



هذه الخطوات لا داعي لها اذا كان الجهاز جزء من دومين معين، حتى لو تم تغيير الدومين فان علامة الصح في الصورة اعلاه تقوم تلقائيا بتغيير اسم الدومين الى الدومين الحالي.

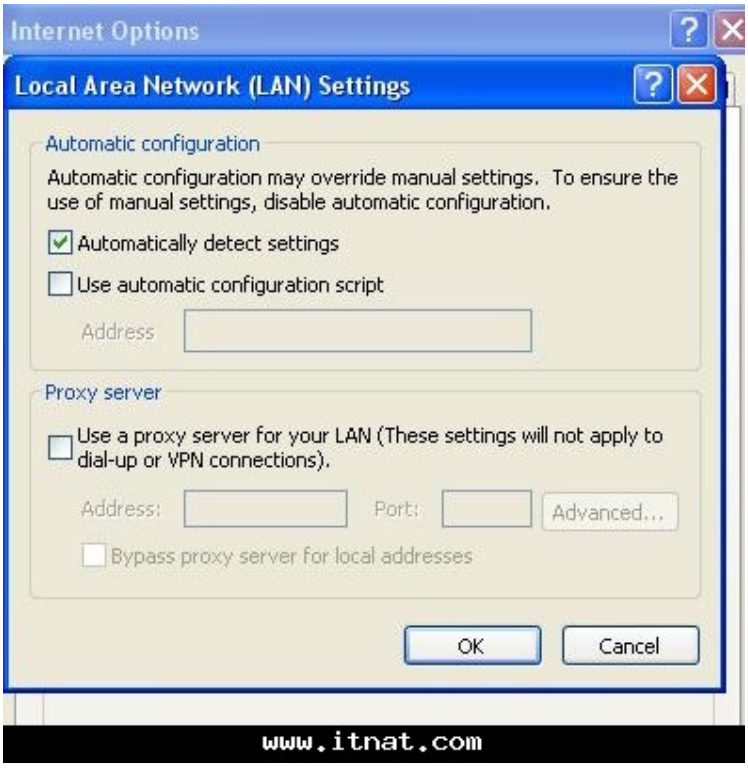
ملاحظه: اذا كان المستخدم يعمل على اكثر من دومين فانك تحتاج الى تعريف اسم ال wpad (CNAME) على كل دومين حتى تضمن توافقه مع ال DNS.

اعداد متصفح المستخدم للاستفاده من خاصيه الاكتشاف الالي(Auto Discovery)

-1اختار خصائص من الانترنت اكسبلورر اما بالضغط باليمين على الايقونه، او اختيار خصائص من داخل المتصفح.

-2اذهب الى لسان الوصلات Connections واختار خصائص الشبكه المحليه.Lan Settings

-3الان ضع علامة صح على Automatically Detect Settings واضغط.OK



وهكذا نكون انتهينا من هذا الدرس الذي تعلمنا فيه كيفية ربط الايزا فايروول مع ال DNS و DHCP حتى يتم التعرف اليه اوتوماتيكيا وبسهوله.

الدرس الخامس:
تحميل ايزا 2004 على ويندوز 2003

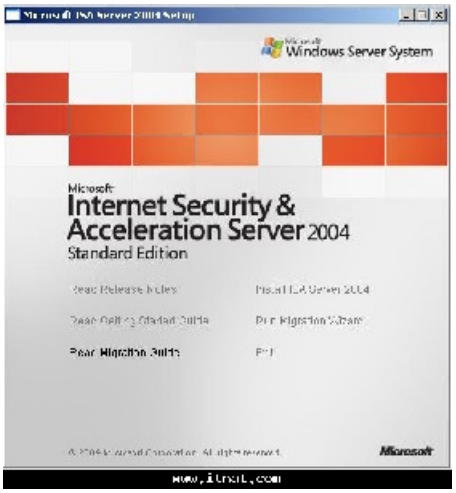
سنتعرف في هذا الدرس على كيفيه تنصيب الايزا 2004 على ويندوز سيرفر 2003 ، يمكنك العوده الى دورة سيرفر 2005 للمزيد عن تنصيب ويندوز سيرفر 2003، بشكل عام تنصيب الايزا مباشر وهناك القليل من القرارات التي يجب ان تتخذها اثناء التنصيب، اهم نقطة يجب الاهتمام بها اثناء التنصيب هو عمليه تحديد نطاق عناوين ال .IP (IP Addresses)

على الاختلاف مع ايزا 2000 فان الايزا 2004لا يستخدم جدول العناوين المحليه (LAT) لتحديد الشبكات الامنه وغير الامنه، الفايروول التابع للايزا 2004 يطلب عناوين الاي بي التي تحدد كيان الشبكه وتعرف بالشبكه الداخليه.
حيث تحتوي الشبكه الداخليه جميع الخدمات والسيرفرات مثل نطاق ال Active Directoryو DNS DHCP RADIUS WINSومحطة ادارة الفايروول وغيرها من خدمات الشبكه المحليه التي يحتاج الفايروول الى التعامل معها مباشره بعد الانتهاء من التنصيب.
الاتصال بين الشبكه الداخليه وفايروول الايزا يتم تحت سيطرة سياسه النظام (System Policy) وهي عباره عن قواعد للعبور معرفه مسبقا تحدد نوع الاتصال بين الشبكه الداخليه والخارجيه، هذه السياسه يمكن اعدادها لتناسب متطلبات الشبكه . سوف تتعامل بشكل مكثف مع السياسه هذه في سبيل تحديد شكل وطريقه الاتصال في شبكتك.

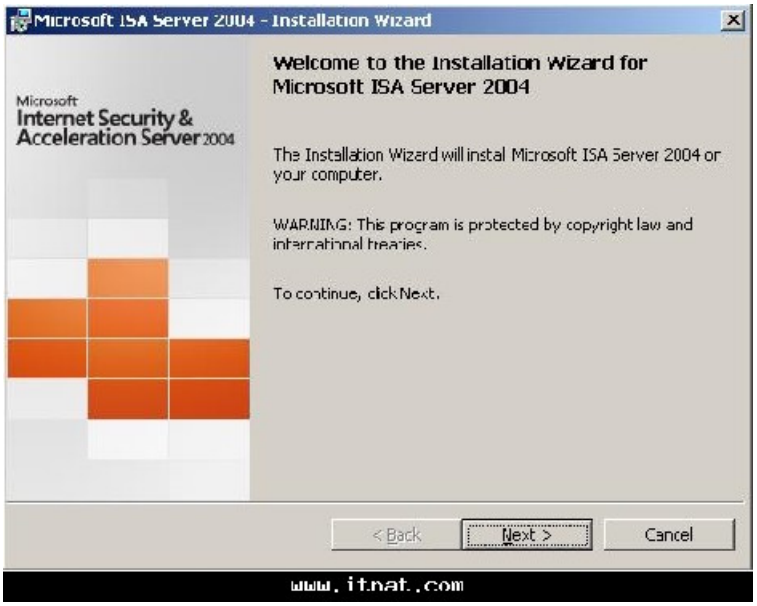
تنصيب الايزا 2004

كما ذكرنا فان تنصيب الايزا 2004 على ويندوز سيرفر 2003 مباشر وصريح، الخطوة الرئيسيه هي تحديد مجموعة عناوين الاي بي التي ستكون للشبكه الداخليه وهو شيئ مهم لان الفايروول سيتعامل معها عند تطبيق سياسه النظام.

الى الخطوات
1-ادخل قرص الايزا لتظهر قائمة التشغيل التلقائي.

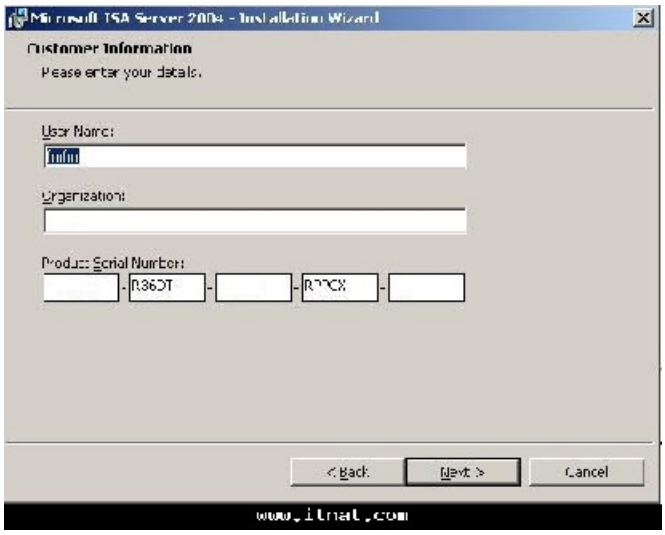


-2اضغط علىInstall ISA Server 2004 ستظهر نافذه ترحيبيه اضغط التالي

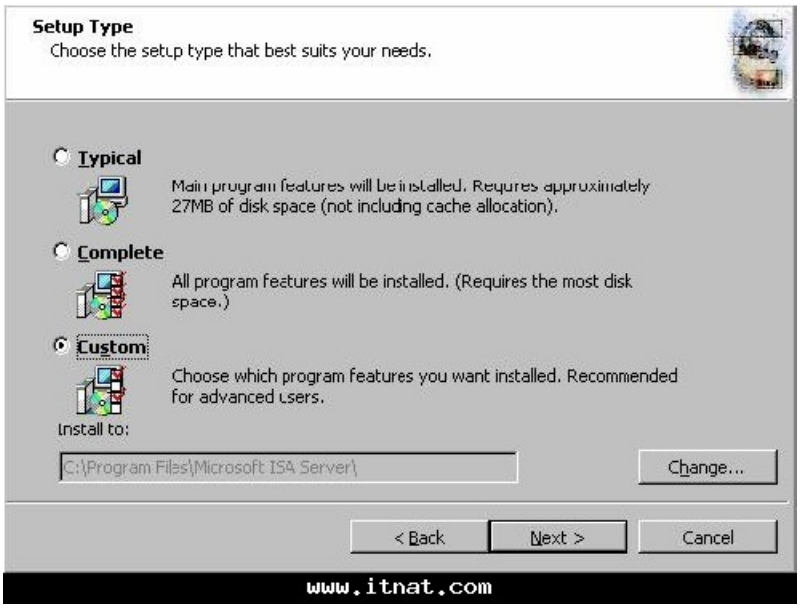


-3اضغط على موافق على الشروط (بعد قرائتها طبعا(

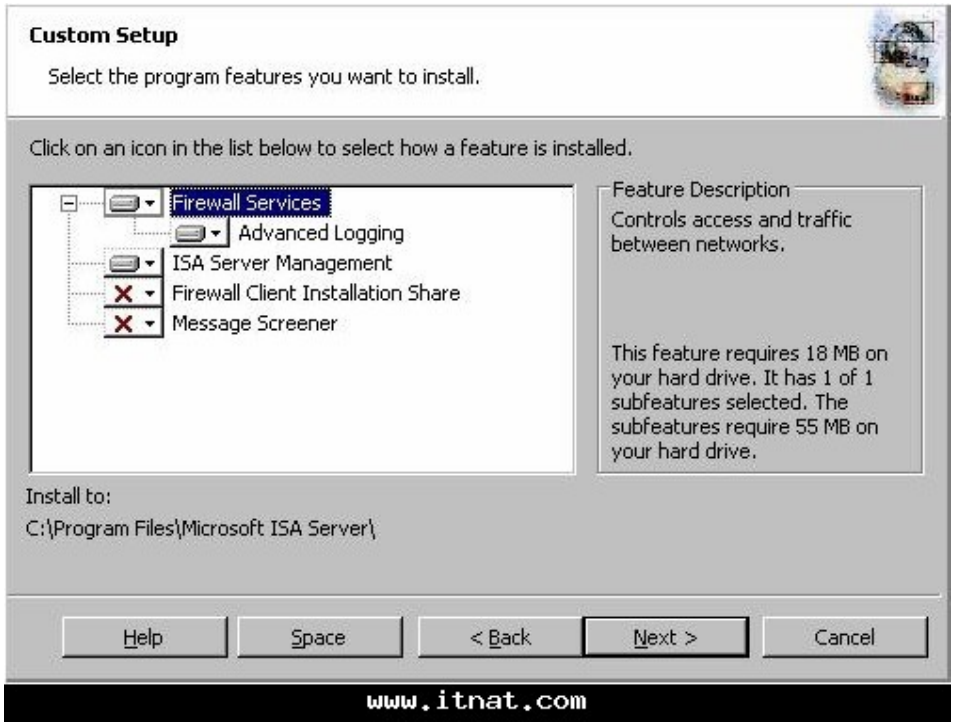
-4في صفحة المعلومات ادخل اسم المستخدم واسم المؤسسه ورقم ترخيص البرنامج.



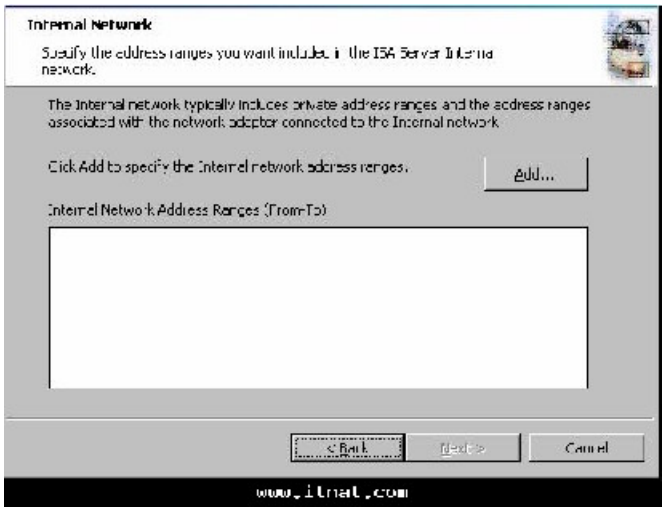
-5في صفحه الاعداد اختار الاعدادات المخصصه Custom ، اذا اردت تغيير مكان التنصيب عن القرص C بامكانك تغييره الان بالضغط على تغيير



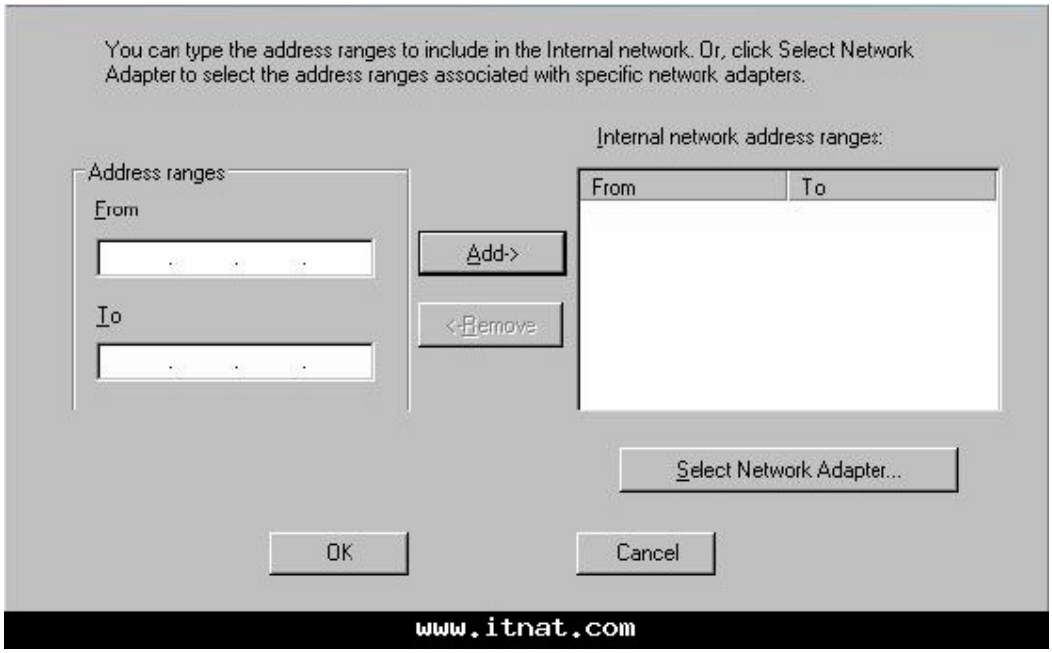
-6الصفحه التاليه ستظهر المكونات التي تريد تنصيبها من عدمه، لاحظ ان الفايروول وادارة الايزا تكون جاهزة للتنصيب بشكل تلقائي، مظهر الرسائل (Message Screener) و Firewall Client Installation Share لا يتم تنصيبهم تلقائيا – يستخدم مظهر الرسائل لمنع السبام من الدخول او الخروج من الشبكه- لتنصيب خدمة مظهر الرسائل يجب تنصيب خدمه IIS 6.0 SMTP ، استمر بدون تغيير اي شيئ في محتويات التنصيب.



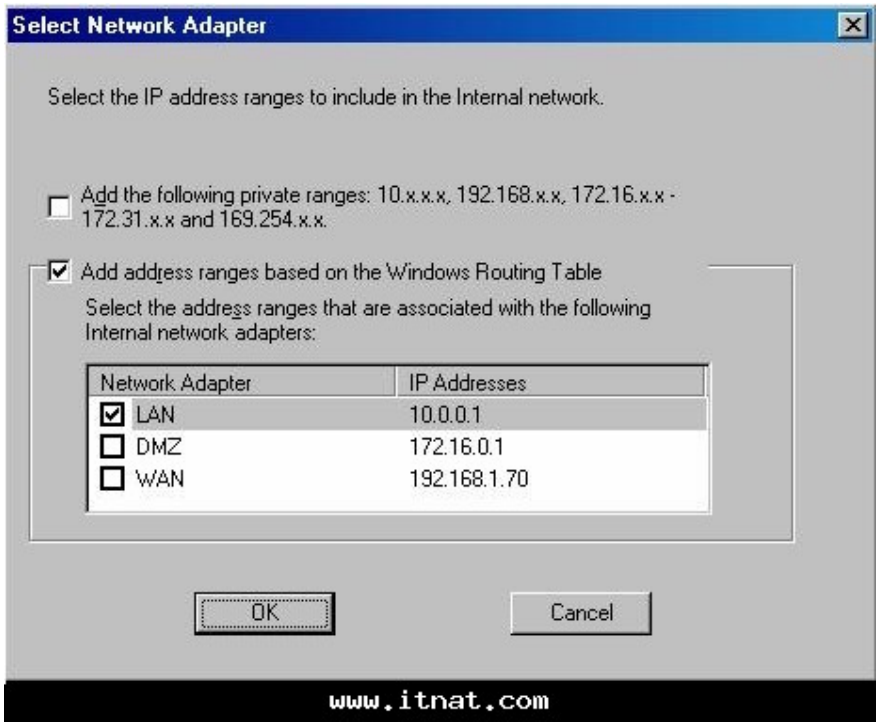
-7الان ستظهر نافذخ تحديد العناوين الداخليه، لمن عمل مع ايزا 2000 هنا الوضه مختلف كما ذكرنا قبل قليل حيث اننا لا نستخدم LAT لان الايزا يحتاج الى الارتباط مع جميع خدمات الشبكه، اضغط علىAdd



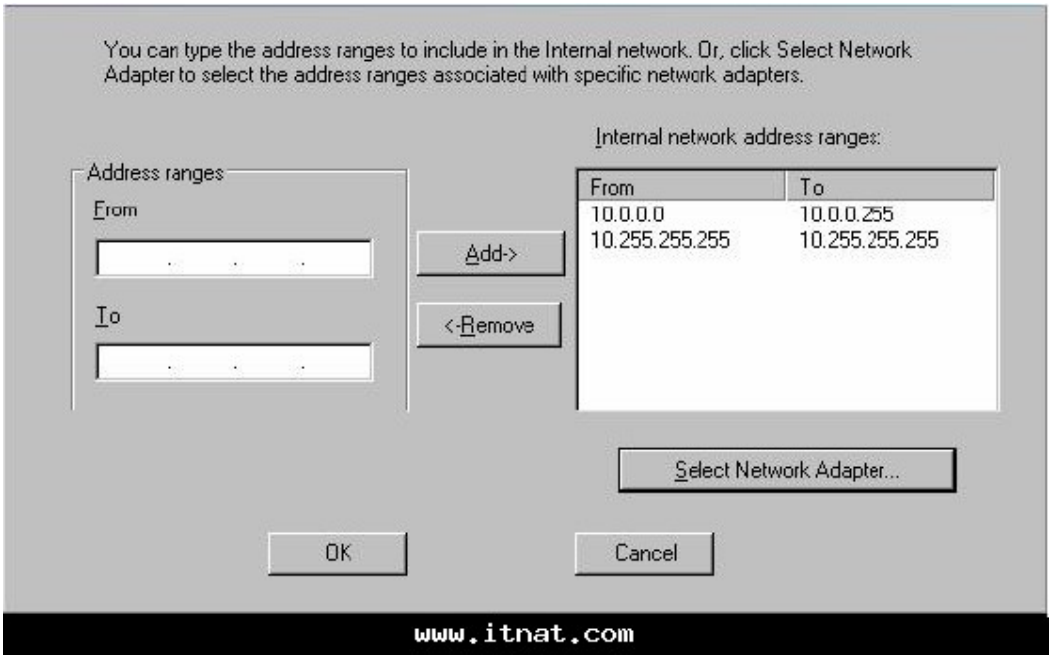
-8الان في نافذه اعداد الشبكه اختارSelect Network Adapter



-9في مربع الحوار قم بازاله الصح من مربع Add the following private range ودع الصح في مربع Add address range based on the windows الان ضع صح في مربع الخاص بكرت الشبكه المتصل بالشبكه الداخله اضغط اوكي

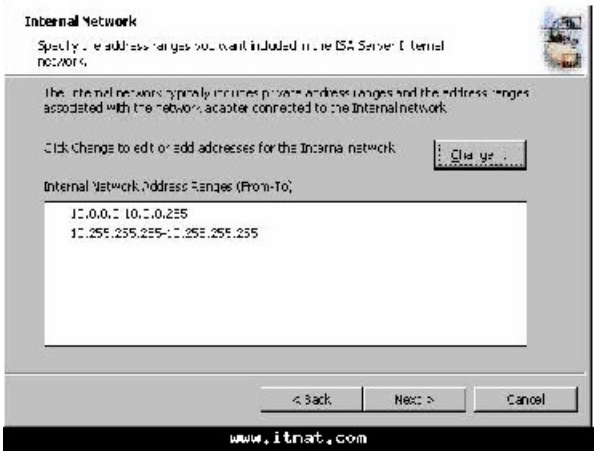


-10ستظهر رساله تؤكد ان الشبكه الداخليه تم تعريفها اضغط اوكي

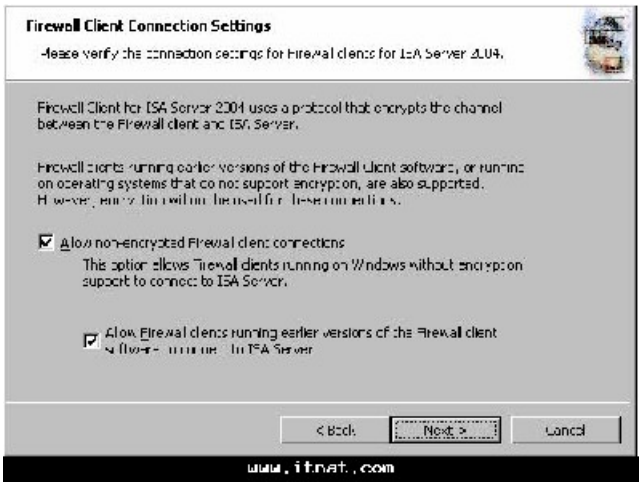


-11اضغط اوكي في مربع حوارInternal Network Address Range

-12اضغط التالي



-13في صفحة اعداد الفايروول ضع صح على الخيارين، هذان الخياران يسمحان اي مستخدم بالاتصال بالايزا حتى لو كان يستخدم نسخه اقدم من نظام التشغيل او من عميل الايزا.



14-في صفحة الخدمات اضغط التالي

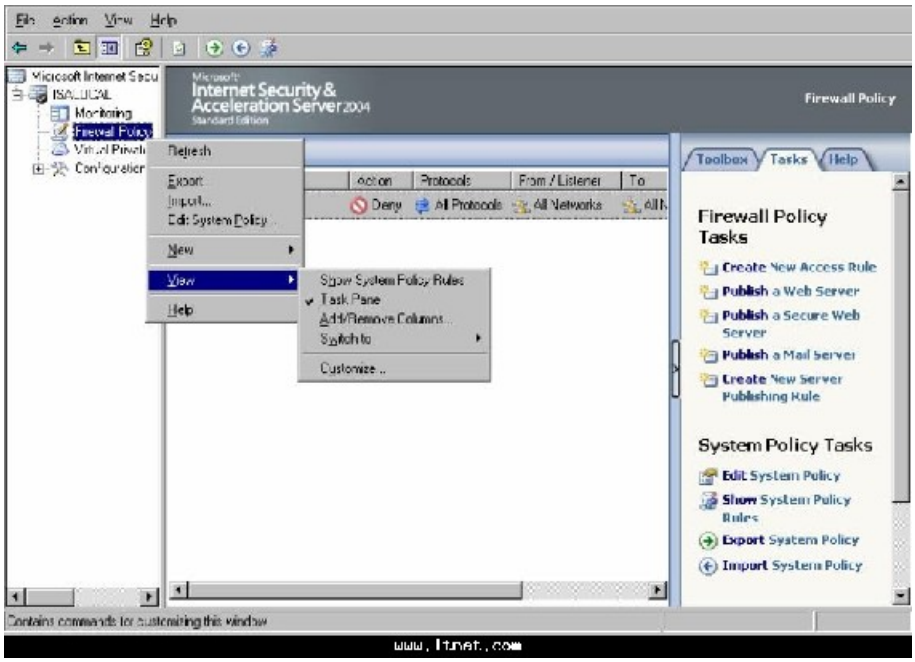
15-الان اضغط على تنصيب لتبدا عمليه التنصيب ثم يتم اعادة التشغيل.

معاينة سياسة النظام

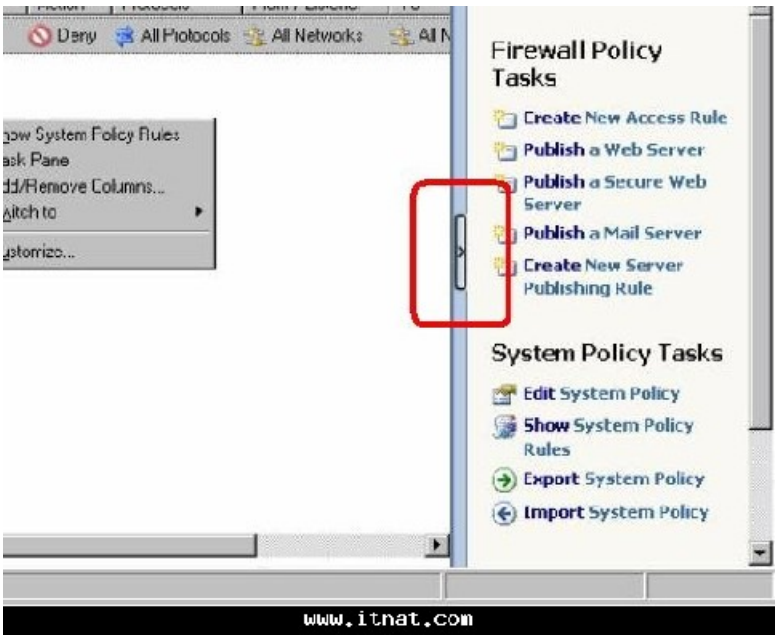
بشكل اساسي فان الايزا بعد تنصيبه لا يسمح لاي شبكه محميه بالوصول الى الانترنت ولا يسمح لاي مضيف من الانترنت بالوصول الى اي جزء من الشبكه المحميه بالفايروول، طبعا هذا يمكن تغييره.

قم بالخطوات التاليه لمعاينة سياسة النظام الحاليه:

1-اضغط علىStart>All Programs> MS ISA server> ISA server management



2-سيظهر كونسول ادارة الايزا، الان اضغط على اسم السيرفر يظهر القائمه التابعه له ثم اضغط على Firewall Policyباليمين ثم اختار Show System Policy Rules منview



-3الان اضغط على السهم على اليمين ليظهر لائحة المهام) Task Pane سهر ازرق صغير) في هذه الائحه تجد ترتيب للمهام بشكل يمثل نقله عن الايزا 2000 حيث انه يساعدك على عمل سياسة النظام بشكل اكثر منهجيه ونظاميه من قبل. النظام يقدملك سياسات اسايه للنظام، في حال استخدامها فانها تبقى اول سياسات يتم تطبيقها قبل اي سياسات تقوم انت بتطبيقها . استمر بالنزول الى قائمه System Policy Rules تجد ان ال Rulesمعرفه ب

Order Number

Name

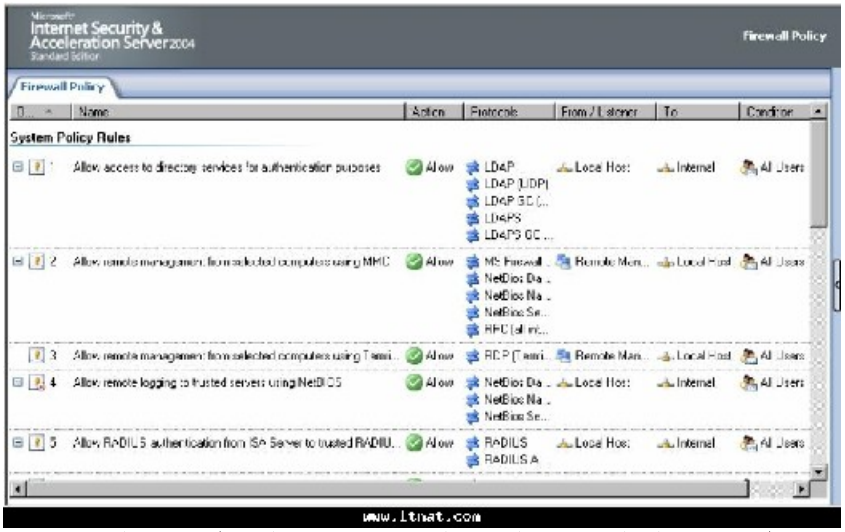
) Actionالسماح او الرفض(

Protocols

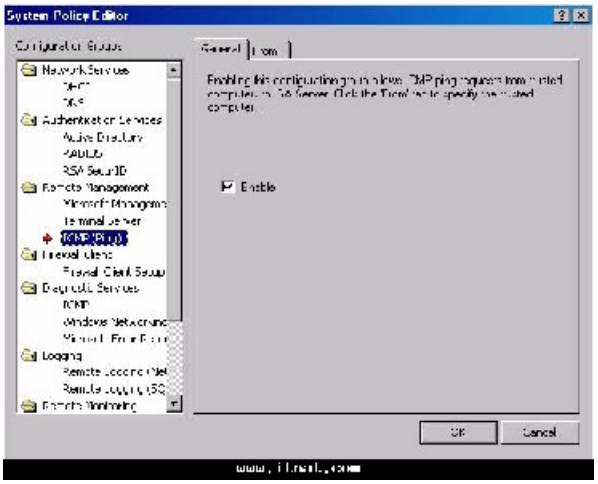
) Fromالشبكه او المستخدم المصدر(

) Toالشبكه او المستخدم المستهدف(

) Conditionمن وماذا ينطبق عليه من هذا الرول(



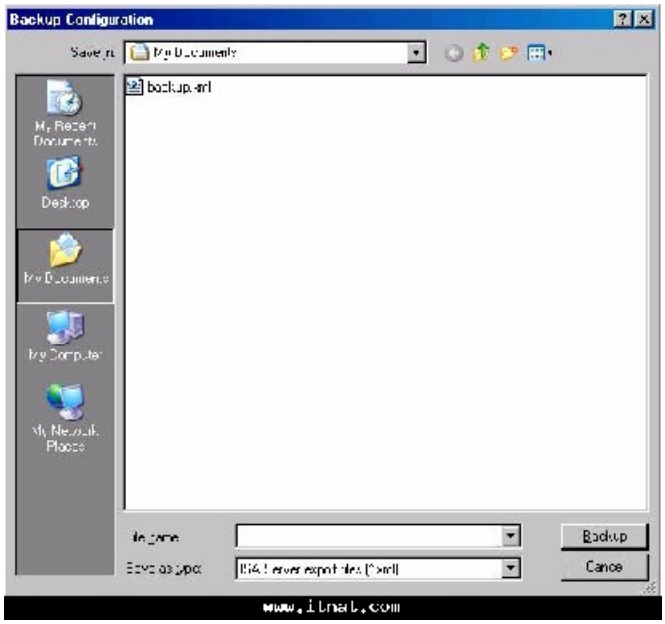
-4لاحظ ان بعض الرولز غير مفعله، يمكنك تغيير وضعها بالضغط مرتين عليها



رمز:
1السياسه موقفه حتى يتم تفعيل وصلةVPN
2هذه السياسات موقفه حتى يتم تفعيل وصله vpn بين موقع وموقع
3هذه السياسه موقفه حتى يتم تفعيل وصلهHTTP/HTTPS
4هذه السياسه موقفه حتى يتم تفعيل فلتر
5هذه السياسه يتم تفعيلها يدويا
6هذه السياسه موقفه اساسا
7هذه السياسه موقفه اساسا
8يتم تفعيل هذه السياسه عند تنصيبFirewall share client
9هذه السياسه موقفه اساسا

الان تستطيع التغيير بالسياسات لتناسب احتياجاتك من حركه داخليه وخارجيه. ينصح بشكل عام ان تقوم بعمل حفظ للاعدادات الاساسيه حتى تستطيع استرجاع الحاله الاساسيه للايزا في حال حدوث اي مشاكل.
عمل حفظ لاعدادات ما بعد التنصيب
-1افتح كونسول ادارة الايزا ثم اضغط باليمين على اسم السيرفر واختارBack up

-2سيظهر مربع يطلب منك ادخال مكان الحفظ سميه باي اسم وتذكر الاسم والمكان ثم اضغط علىbackup



-3سيظهر مربع حوار يطلب منك ادخال كلمة سر ، الهدف منها حمايه الباك اب لانه يحتوي الكثير من المعلومات المهمه عن المستخدمين وعن اعدادات الشبكه.

-4اضغط اوكي لانهاء عمليه الباك اب
تذكر ان تنقل الحفظ الى مكان خارج الشبكه يدعم نظام NTFS بسبب وجود التشفير عليه.

هكذا نكون تعرفنا على طريقه تنصيب الايزا 2004 على ويندوز سيرفر 2003 وتعرفنا على الاعدادات الاساسيه لضمان الاتصال الداخلي والخارجي بالشبكه.

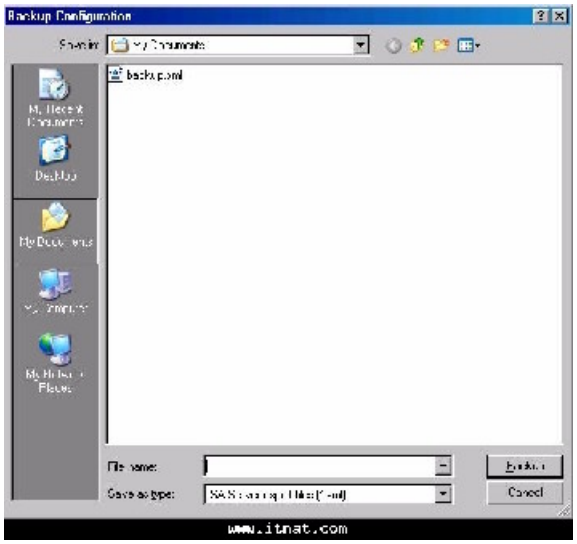
الدرس السادس:
طريقة عمل باك اب واسترجاع اعدادات الآيزا بصورة صحيحة- أيزا2004

ملخص :يتميز الايزا 2004 عن الاصدار السابق بان ميكانيكيه الباك اب وحفظ الاعدادات تسمح لك باسترجاع الاعدادات بشكل كامل او جزئي الى الايزا 2004 على نفس الجهاز او على جهاز اخر مما يمكنك من الاستفاده بشكل كامل من الباك اب في حال حدوث مشاكل تستدعي تغيير السيرفر او نظام التشغيل .

عملية الباك اب يفضل ان تتم بعد حدوث واحد او اكثر من العمليات التاليه:
-تغيير حجم الكاش او مكانها
-تغيير سياسة الفايروول
-تغيير قاعده الرول
-تغيير رول النظام
-تغيير على الشبكه من اسم او رول
-اعطاء او سحب صلاحيات اداريه من المستخدمين
يفضل ايضا عمل باك اب بعد تنصيب الايزا، هذا الاجراء يساعدك في استرجاع الحاله الاصليه للايزا بدون المرور في اجراءات اعادة تنصيبه من البدايه
عمليه الباك اب لاعدادت الفايروول التابع للايزا 2004

-1افتح كونسول ادارة الايزا واضغط باليمين على اسم السيرفر ثم اختارBack up

-2سوف يظهر مربع حوار ادخل اسم ملف الباك اب وانتبه الى مكان حفظ الباك اب ثم اضغط علىbackup

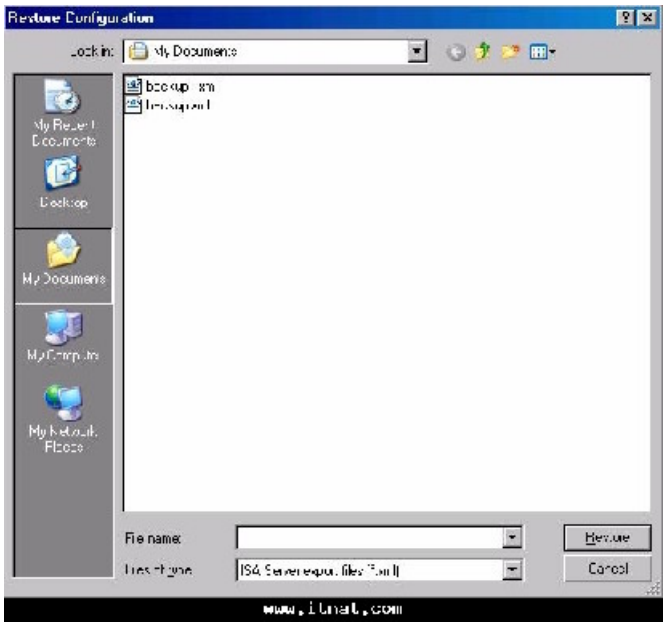


-3ادخل الباسوورد في مربع الحوار التالي، الغرض من الباسوورد كما ذكرنا في الدرس السابق هو ان اعدادات الايزا قد تحتوي على معلومات مهمه عن المستخدمين وعن الشبكه.

-4اضغط اوكي حتى تتم عمليه الباك اب
استعادة الاعدادات من ملف الباك اب

-1افتح كونسول ادارة الايزا واضغط على باليمين على اسم السيرفر ثم اختارRestore

-2سوف يظهر مربع حوار اذهب الى حيث خزنت ملف الباك اب واضغط على زرrestore

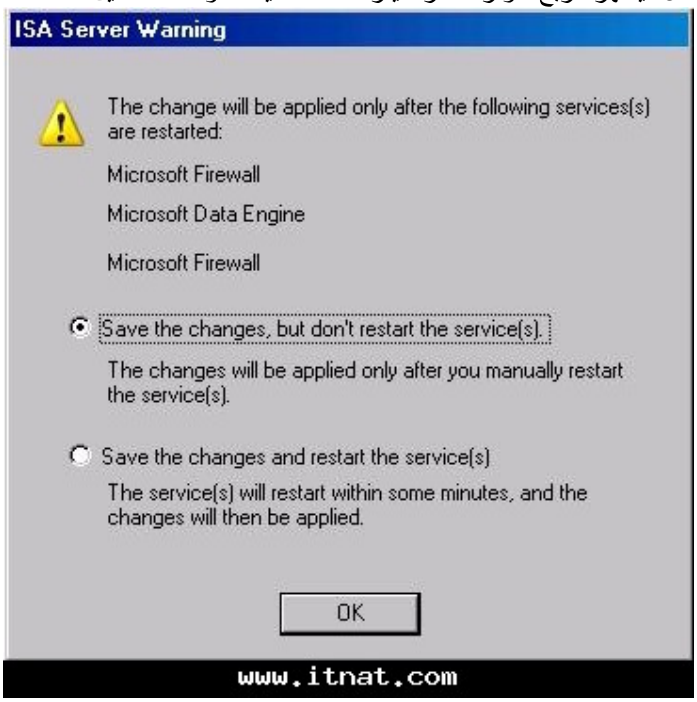


-3ادخل الباسوورد

-4اضغط اوكي لتبدا عمليه الاسترجاع

-5اضغط على Apply لحفظ التعديلات على سياسه الفايروول

-6سيظهر مربع حوار اختار خيار حفظ التعديلات واعادة تشغيل الخدمات حتى يتم تطبيقها



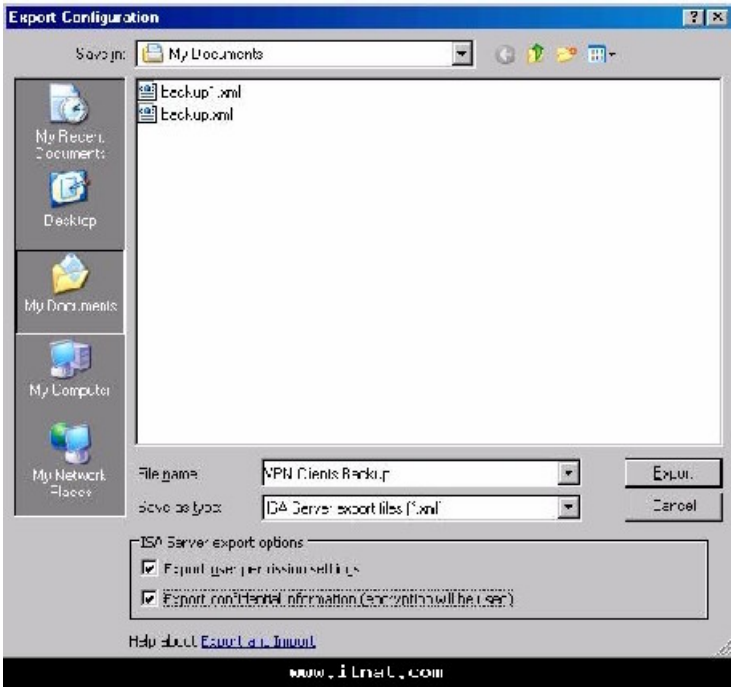
تصدير سياسة الفايروول

في بعض الاحيان قد لا تحتاج الى استعاده جميع الاعدادات، مثلا قد تصادف مشكله في سياسه الوصول، وتحتاج الى مساعده احد فتقوم بعمل باك اب للاعدادت وارسالها اليه حتى يستعيدها على جهاز فحص، يمكنك فعل هذه العمليه بسهوله عن طريق خيار. Export Configuration

في هذا المثال سنفترض اننا نريد تصدير اعدادت عملاء VPN كالتالي:

-1افتح كونسول اداره الايزا افتح السيرفر حتى تظهر علامة VPN ثم اضغط عليها باليمين واختار Export VPN Clients Configuration .

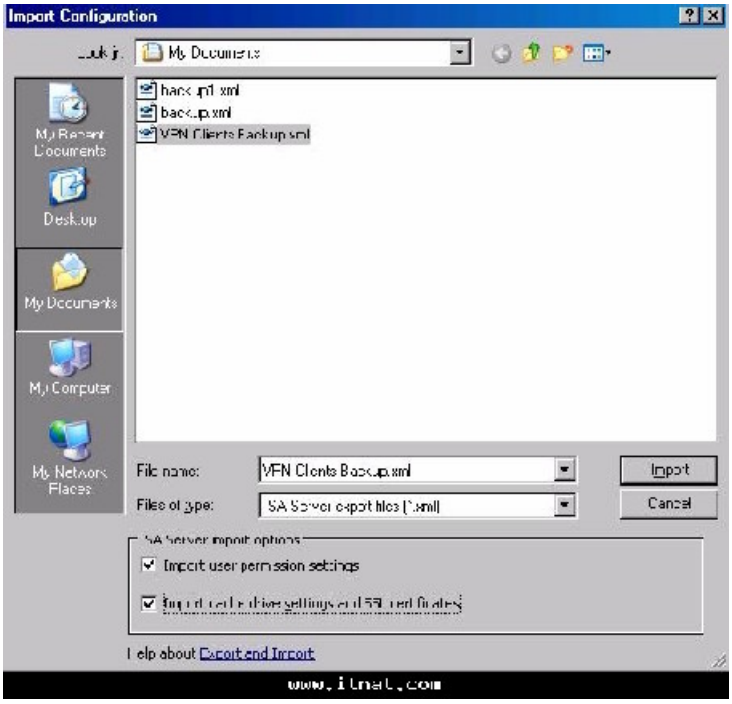
-2سيظهر مربع حوار ادخل اسم ومكان تخزين ملف الاعدادات لاحظ الخيارين بالاسفل اختار ما يناسبك، في حالتنا سنختار هما الاثنان.



-3بعد الضغط على Export سيطلب منك باسوورد

-4اضغط اوكي لتتم عمليه التصدير المحدده
استيراد سياسة الفايروول
الان سنقوم باستيراد اعدادت ال VPN التي قمنا بتصديرها قبل قليل
-1افتح كونسول ادارة الايزا افتح السيرفر حتى تظهر علامة VPN ثم اضغط عليها باليمين واختار Import VPN Clients Configuration .

-2في مربع الحوار اختار الملف من مكان ما خزنته وضع صح على الخيارين ثم اضغط استيراد



-3ادخل الباسوورد التي قمت بادخالها سابقا

-4اضغط اوكي ثم Apply ليتم تطبيق الاعدادات الجديده التي قمت باستيرادها من الجهاز السابق.
هكذا تعلمنا كيفيه عمل باك اب واستعادة للاعدادات بشكل كامل او تفصيلي مع العلم ان طريقه ال VPN يمكن ان تطبق على اي عنصر من عناصر الايزا2004.

الدرس السابع:
اعداد سياسات الوصول للايزا Access Policy 2004

ملخص :في هذا الدرس سنناقش اهم ميزه في الايزا 2004 وهي عملية تحديد سياسات الوصول Access Policyوفيها تسطيع التحكم الكامل بالاتصالات الداخله والخارجه لشبكتك لتامين اكبر قدر من الحمايه والامن والتحكم .

اصبح معروف الان ان الفايروول الخاص بالايزا 2004 يتحكم بالاتصالات بين الشبكات المتصله به، عند تنصيب الايزا فانه يكون في وضع يمنع جميع الاتصالات، الطرق المستخدمه للسماح بالاتصالات عن طريق الفايروول هي:

-قواعد الوصول Access Rules
-قواعد النشر Publishing Rules

قواعد الوصول تتحكم بالوصول من شبكه محميه الى شبكه غير محميه. في مفهوم الايزا فان جميع الشبكات ما عدا الشبكه الخارجيه هي شبكات محميه. وكل الشبكات الخارجيه هي شبكات غير محميه.
الشبكات المحميه تشمل عملاء VPN والشبكه المحليه والشبكه الداخليه وشبكه المحيط. الانترنت يعتبر شبكه خارجيه لكن ايضا يمكن اعتبار الشبكات المرادفه خارج نطاق الشبكه المحليه والتي يمكن للعملاء ان يتصلوا بها ، يمكن ان تعتبر شبكات خارجيه.
بالنسبه لقواعد النشر فانها على العكس من قواعد الوصول تسمح لمضيف على شبكه خارجيه بالوصول الى اي مصادر على الشبكه الداخليه، مثلا شركه تريد عمل استضافه لموقعها مع خدمه ftp وبريد الكتروني، بمساعده قواعد النشر فان اي شخص من الخارج بالصلاحيات اللازمه يستطيع الوصول الى هذه المصادر.
بشكل عام من مواصفات الفايروول القوي هو ان يكون عندك تحكم كامل بقدرات كل مستخدم على الاتصال بالشبكه الخارجيه حتى تستطيع استخدام هذا التحكم بافضل شكل لحمايه الشبكه.
تحتوي قاعدة الوصول على العناصر التاليه

عنصر القاعده	الوصف
الاولويه Order (Priority)	سياسة الفايروول مكونه من عده قواعد وصول، هذه القواعد يتم معالجتها بشكل متسلسل حتى الوصول الى القاعده المطابقه للوصله.
اجراء	هناك اجرائين : السماح او الرفض
بروتوكولات	البروتوكولات الخاصه بالاتصال مثل TCP/IP و ICMP الخ
المصدر	مصدر الاتصال الذي قد يكون عنوان اي بي مفرد او مجموعة عناوين او حتى شبكه جزئيه subnet
المستقبل	مستقبل الاتصال قد يكون دومين واحد او مجموعة عنوان اي بي او عده عناوين شبكه جزيئه او عده شبكات
الشرط	الشرط هو المستخدم او المجموعه التي تنتمي اليها القاعده rule

www.itnat.com

لناخذ مثال على قواعد الوصول حتى نتعرف اكثر عليها

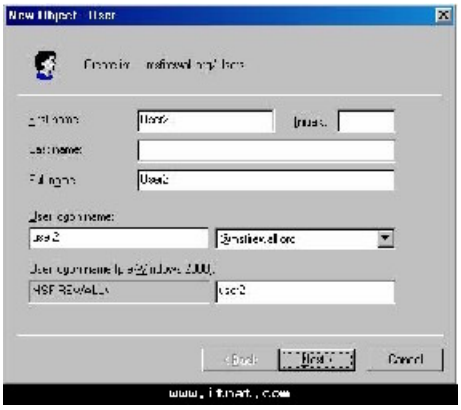
عنصر القاعده	الوصف
الاولويه Order (Priority)	1
اجراء	السماح
بروتوكولات	HTTP و FTP تحميل
المصدر	الشبكة الداخليه
المستقبل	www.microsoft.com and ftp.microsoft.com
الشرط	وصول ويب محدود Limited Web Access

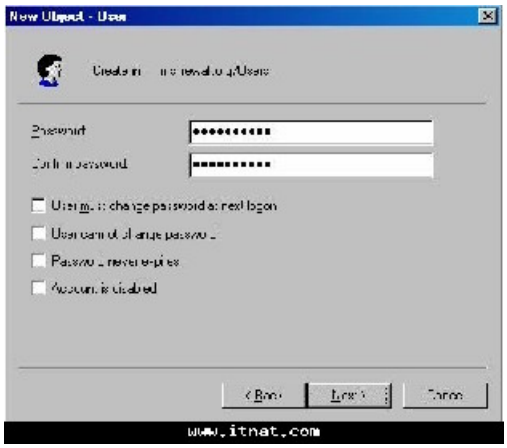
www.itnat.com

هذه القاعده تسمح للمستخدمين من مجموعه Limited Web Access باستخدام بروتوكلات HTTP وFTP ، ايضا اعضاء المجموعه يجب ان يكونوا اعضاء من الشبكه الداخليه ويسمح لهم بالاتصال مع المواقع المسجله في المستقبل.
سنتعلم في هذا الدرس انشاء عدة قواعد وصول للتحكم بالوصول الخارجي عن طريق الايزا 2004

اولا ننشئ مستخدم جديد

نقوم بانشاء مستخدم بالاكتيف دايركتوري تحت اسم
user2





في حال انك استخدمت network templates سنقوم بوقف قواعد الوصول الخاصه بها (وقف فقط لاننا سنستخدمها لاحقا)
لوقف هذه القواعد قم بالتالي

1-افتح كونسول ادارة الايزا وافتح اسم السيرفر ثم اضغط على عقدة
Firewall Policy

2-الان ستظهر في نافذه التفاصيل اسماء القواعد قم باختيارها جميعا ثم باليمين اختار
Disable

3-اضغط على تطبيق لحفظ التغييرات

4-اضغط على اوكي للتاكيد

انشاء قاعدة وصول لتحديد البروتوكلات والمواقع التي يستطيع المستخدمين الوصول اليها

اول قاعدة وصول سوف تحدد وصول المستخدمين فقط الى بروتوكولات HTTP و HTTPS بالاضافه الى تحديد استخدام هذه البروتوكولات الى مواقع مايكروسوفت.
سيتم انشاء مجموعة اسمها Limited Access Web Users ثم نضيف للمستخدم الذي قمنا بانشاءه الى هذه المجموعه
قاعدة الوصول ستكون كالشكل التالي

عنصر القاعده	الوصف
الاولويه Order (Priority)	3 (بعد ن يتم انشاء كل القواعد)
الاسم	Limited Access Web Users
اجراء	لسماح
بروتوكولات	HTTP و HTTPS
المصدر	لشبكة الداخليه
المستقبل	نطق مايكروسوفت
الشرط	مجموعة Limited Access Web Users

www.itnat.com

ستظهر القاعده كالصورة التاليه

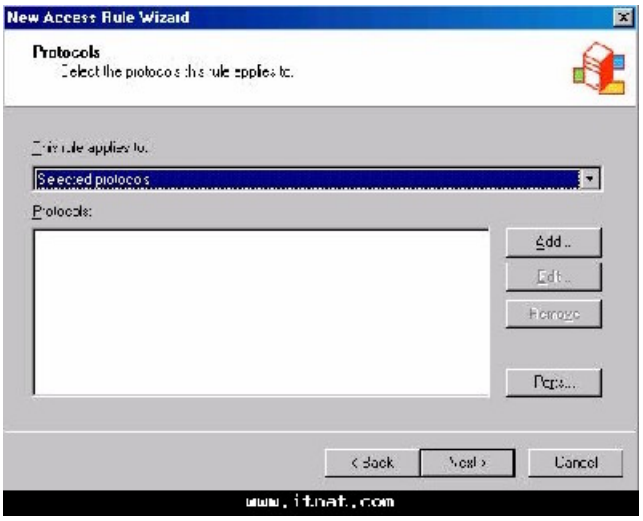
الان نفذ الخطوات التاليه لانشاء قاعدة وصول

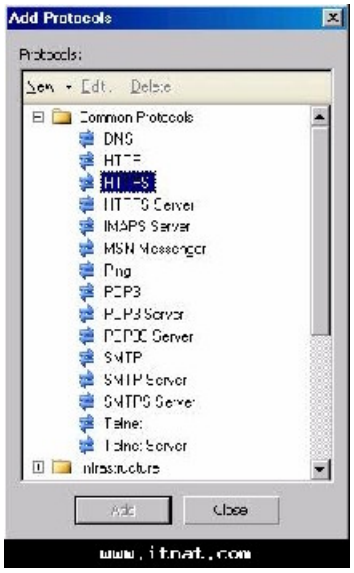
1-افتح كونسول ادارةالايزا ثم افتح اسم السيرفر واضغط على عقدة ال Firewall Policyسيظهر لسان المهام Tasksعلى اليمين اضغط عليه ثم على انشاء قاعدو وصول جديده كما في الصورة.

2-الان سيظهر مربع حوار لانشاء القاعده الجديده، سيبدا بالاسم ادخل الاسم Limited Users Web Access اضغط التالي

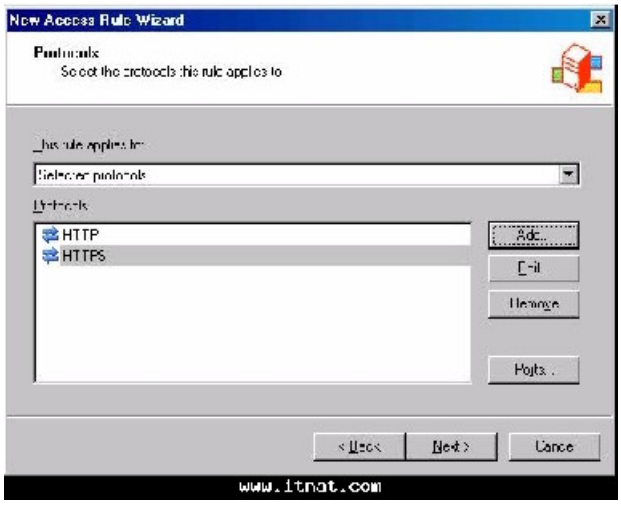
3-اختار السماح في اجراء القاعده

4-في صفحة البروتوكولات اختار هذه البروتوكولات من القائمه المسندله ثم اضغط على اضافه لاضافة البروتوكولاتHTTP و HTTPS

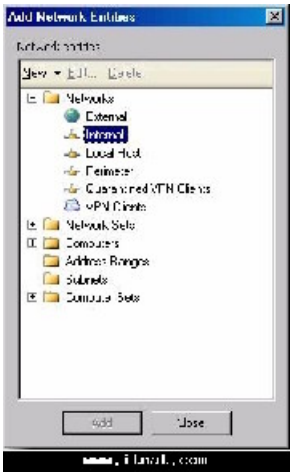




-5اضغط التالي

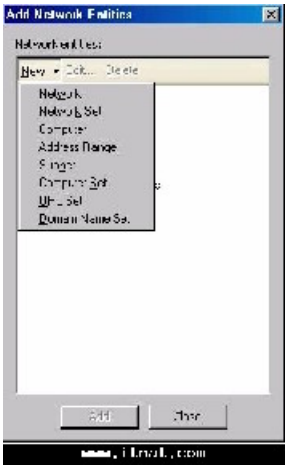


-6في صفحة مصدر قاعدة الوصول اضغط على اضافه ثم اختار الشبكه الداخليه كما في الصورة.

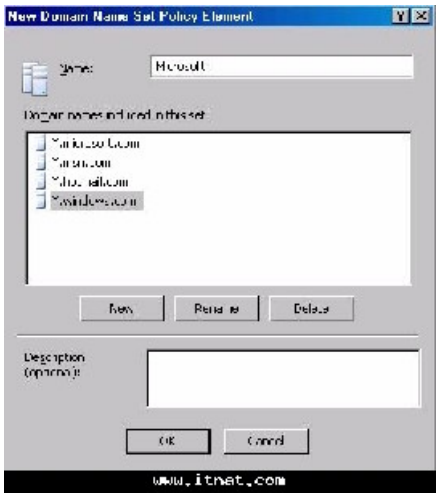


-7اضغط التالي

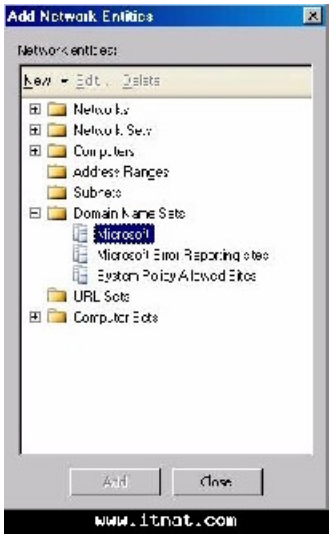
-8في صفحة المستقبل اضغط على اضافه ثم اختار كيان جديد واضغط علىDomain Name Set



-9في مربع الحوار الخاص باسم النطاق اضغط على جديد ثم ادخل اسم النطاق الاول *.microsoft.com اضغط انتر. الان ادخل الاسامي التاليه *.msn.com و *.hotmail.com و *.windows.com في مربع الاسم ادخل Microsoft واضغط اوكي.



-10الان سيظهر مربع اضافه الشبكات اختار مجلد الدومين ثم اضغط على ادخال مايكروسوفت الذي قمنا بانشائه في الخطوة السابقه ثم اغلق النافذه.



-11الان في صفحة المستخدمين اختار ادخال All Users وقم بحذفه ثم اضغط على اضافه
-12في مربع حوار اضافه مستخدمين اضغط على جديد

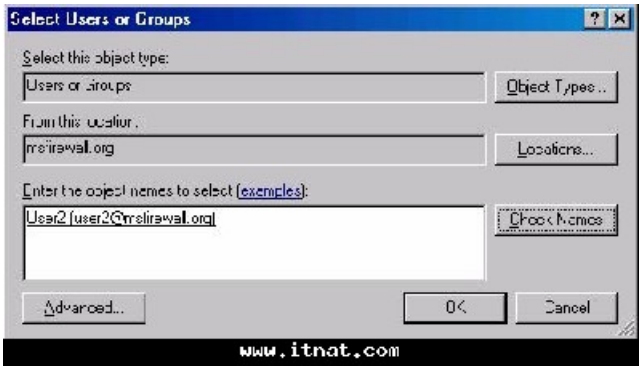
-13ستظهر نافذه جديده لاضافه مستخدمين جدد، الان ادخل اسم مجموعة المستخدمين المستهدفه وهي Limited Web Usersواضغط التالي

-14في صفحة المستخدمين اضغط على اضافه ثم اختار خيارWindows Users and Groups

-15في اختيار المستخدمين اضغط على زر Location

-16سيظهر مربع حوار المواقع مدد الفهرس كامل واضغط على اسم نطاقك (في مثالنا firewall.org) ثم اضغط اوكي.

-17الان سيظهر مربع جديد لاختيار المستخدمين ادخل اسم المستخدم الذي قمنا بانشائه User2 وحدد خيار التاكد من الاسم ليقوم الاكتيف دايركتوري بالتاكد من الاسم ثم اضغط اوكي.



-18اضغط التالي

-19اضغط انهاء لتكون حددت المستخدمين

-20اضغط مرتين على ادخال Limited Web Users في مربع اضافه المستخدمين ثم اضغط على اغلاق

-21الان سيظهر ادخال Limited Web Users كالمجموعه التي ستطبق عليها هذه القاعده اضغط التالي

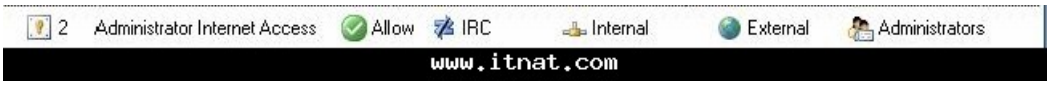
-22اضغط انهاء لاغلاق المعالج.

انشاء قاعده وصول لاعطاء مدراء الشبكه المزيد من المزايا للاتصال

مدراء الشبكه يحتاجون الى مستوى اتصال اعلى من المستخدمين العاديين لاغراض متعدده، لكن مع هذا حتى مدراء الشبكه يجب ان يكونوا محددين من بعض البروتوكولات التي قد تعرض الشبكه للخطر مثل بروتوكول IRCالخاص بالمحادثه الذي يستخدم لتبادل الملفات.
سوف نقوم بانشاء قاعده تسمح لاعضاء مجموعة الادارة بالوصول الى جميع البروتوكولات ما عدا IRC. كما في الجدول التالي

عنصر القاعده	الوصف
الأولويه Order (Priority)	2 (بعد ان يتم انشاء كل القواعد)
الاسم	Administrator Internet Access
جراء	السماح
بروتوكولات	جميعها ما عدا IRC
المصدر	الشبكة الداخليه
لمستقبل	الشبكه الخارجيه
الشرط	مجموعة Administrators

سوف تظهر القاعده كما الصورة



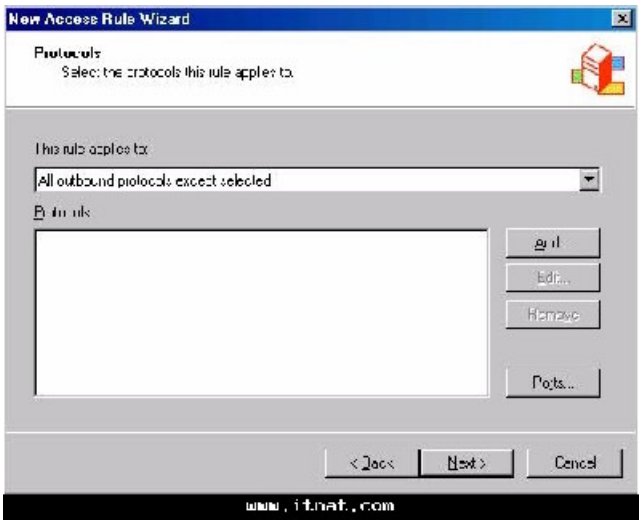
الان الى الخطوات

1-افتح كونسول ادارة الايزا واذهب الى السيرفر ثم الى سياسة الفايروول ثم باليمين واختار new ثم access rule

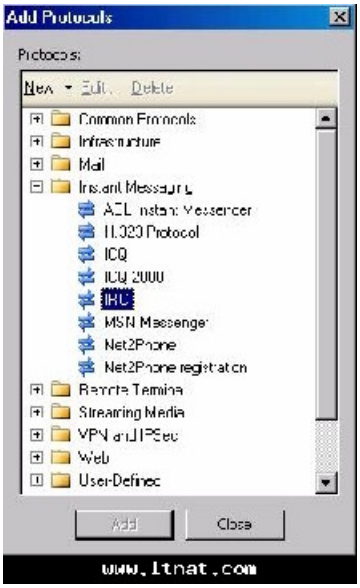
2-في معالج انشاء القاعده ادخل اسمها Administrator Internet Access ثم التالي

3-في صفحة الاجراء اختار سماح

4-في صفحة البروتوكولات اختار من القائمه المنسدله This rule applies to ثم خيار All protocols except selectedثم اضغط على اضافه



-5في مربع اضافه بروتوكول احتار مجلد Instant messaging واضغط مرتين على بروتوكول IRC ثم اغلق المربع



-6اضغط التالي في صفحة البروتوكولات

-7في صفحه مصدر القاعده اضغط على اضافه ثم اضافه كيان شبكه ثم اضغط على مجلد الشبكات واختار الشبكه الداخليه Internal ثم اضغط اغلاق

-8في صفحة قاعده الوصول اضغط التالي

-9في صفحة المستقبل اضغط على اضافه ثم افتح مجلد الشبكات واضغط مرتين على ادخال External اضغط اغلاق .
-10في صفحة المستخدمين اضغط على كل امستخدمين ثم ازاله ، بعدها اضغط على اضافه

11-اضغط على جديد في صفحة اضافه المستخدمين
12-في صفحة معالج المستخدمين الجدد ادخل اسم مجموعة المستخدمين و هو في حالتناAdministrators

13-في صفحة المستخدمين اضغط على اضافه ثم اختارWindows users and groups

14-في اختيار المستخدمين اضغط على زر المواقع

15-في مربع اختيار المواقع مدد الفهرس بالكامل ثم اضغط على اسم النطاق واضغط اوكي

16-في مربع اختيار المستخدمين اختار مدراء النطاق في Enter the object names to select ثم اضغط على التاكد من الاسم ثم اضغط اوكي.

17-اضغط التالي

18-اضغط انهاء لاغلاق معالج اضافه المستخدمين

19-في صفحة اضافه المستخدمين اضغط مرتين على ادخال Administrators ثم اضغط اغلاق

20-اضغط التالي

21-اضغط انهاء لاغلاق معالج انشاء قاعده جديده

انشاء قاعدة وصول للسماح لسيرفر DNS داخلي بالاتصال بسيرفر DNS على الانترنت

سنفترض ان سيرفر DNS على شبكتنا الداخليه يستخدم لمعالجه عناوين الانترنت، هذا السيرفر يجب ان يكون قادرا على معالجة عناوين الانترنت بالاتصال بسيرفرات DNS موجوده على الانترنت.
مع الاخذ بعين الاعتبار ان الكثير من الاجهزة التي تشغل خدمات حساسه للشبكه لا يستخدمها مستخدمين عاديين، سنقوم بانشاء قاعدة بيانات لا تحتاج الى ادخال حساب مستخدم بل تعتمد على انشاء قائمه اجهزة تحتوي سيرفرات DNS على الشبكه. قائمه الاجهزة هو مجموعة من اسامي الاجهزه والعناوين الخاصه بها، تستخدم لتخصيص قاعده وصول للتحكم بالاتصال الى الخارج لهذه الاجهزه. طبعا لتنفيذ هذا الاجراء بسهوله عليك ان تقوم بانشاء مجموعات للاجهزه على الشبكه حسب اختصاص كل جهاز حتى لا تعتمد على دخول المستخدم لتشغيل قاعدة وصول.
قاعدة الوصول ستكون كما الجدول:

عنصر القاعده	الوصف
الاولويه Order (Priority)	1 (بعد ان يتم انشاء كل القواعد)
الاسم	DNS Servers
اجراء	لسماح
بروتوكولات	DNS
لمصدر	DNS Servers
المستقبل	لشبكه الخارجيه
الشرط	جميع لمستخدمين

www.itnat.com

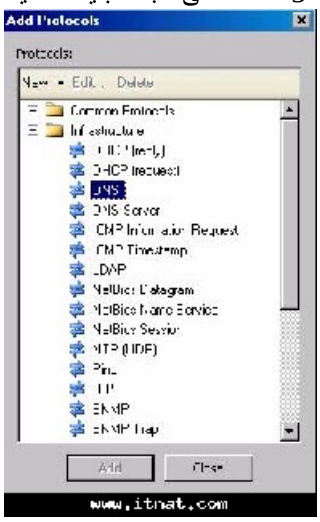
سيكون شكل القاعده كالتالي

الان الى الخطوات:

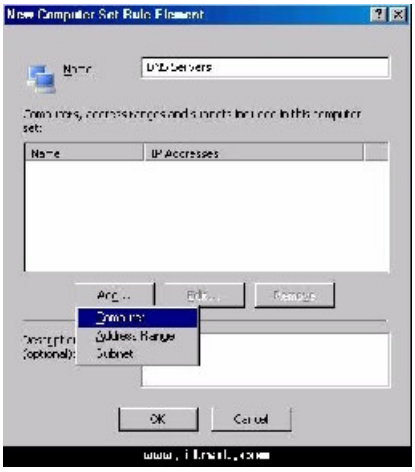
-1افتح كونسول ادارة الايزا، اذهب الى سياسه الفايروول ثم باليمين اختار جديد ثمAccess Rule

-2في معالج انشاء القاعده ادخل اسم القاعده DNS Servers اضغط التالي

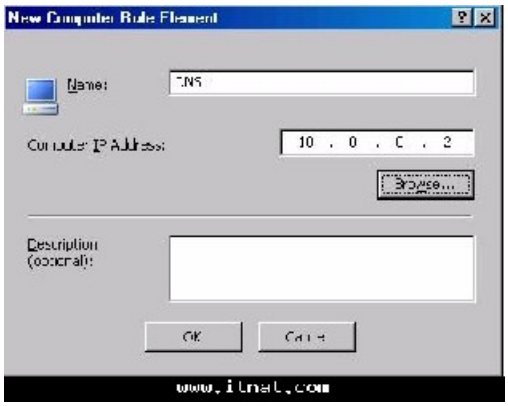
-3السماح في اجراء القاعده ثم التالي
-4في صفحة البروتوكولات اختار من القائمه المنسدله This rule applies to ثم اضغط على اضافه
-5اضغط على مجلد البنيه التحتيه Infrastructure ثم اضغط مرتين على بروتوكولDNS اضغط اغلاق



-6اضغط التالي
-7في المصدر اضغط اضافه ثم جديد ثم اضغط علىComputer Set
-8في مربع حوار مجموعة الاجهزة اضغط على اضافه ثم خيارcomputer



-9في مربع New Computer Rule Element ادخل اسم الجهاز ك DNS1 ثم ادخل عنوان الجهاز واضغط اوكي



-10اضغط اوكي مره اخرى
-11في مربع حوار اضافه كيان الشبكه اضغط على مجلد Computer sets ومرتين على ادخال DNS Serversثم اغلاق

-12اضغط التالي في صفحة مصدر القاعده

-13في صفحة المستقبل اضغط اضافه ثم اضغط على مجلد الشبكات واختار ادخال External ثم اغلاق

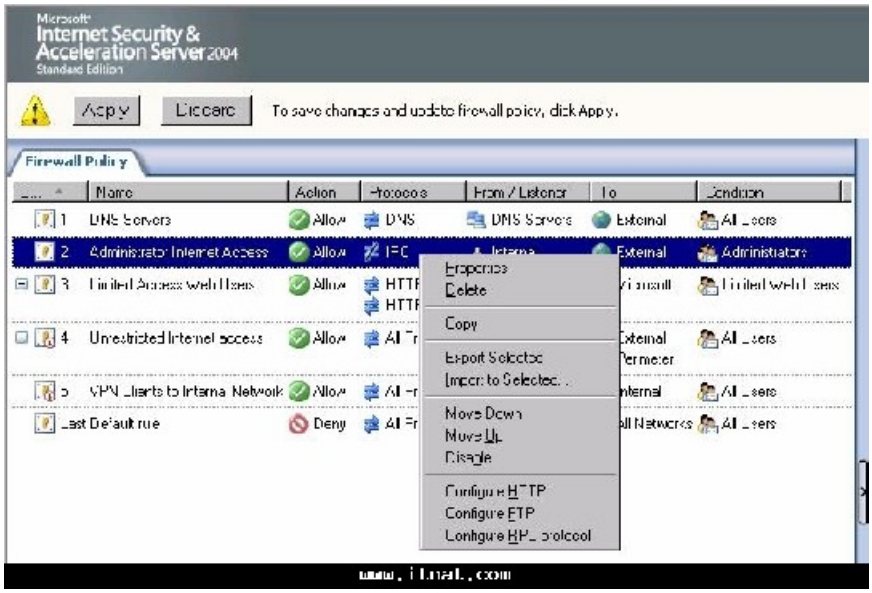
-14اضغط التالي

-15في صفحة مجموعة المستخدمين ندعها كما في ثم نضغط التالي

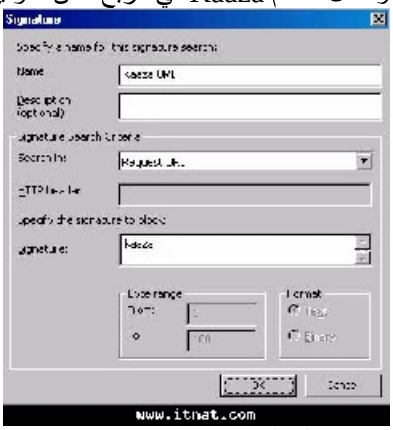
-16اضغط انهاء لنغلق المعالج

استخدام سياسه HTTP لمنع الوصول الى موقع الانترنت

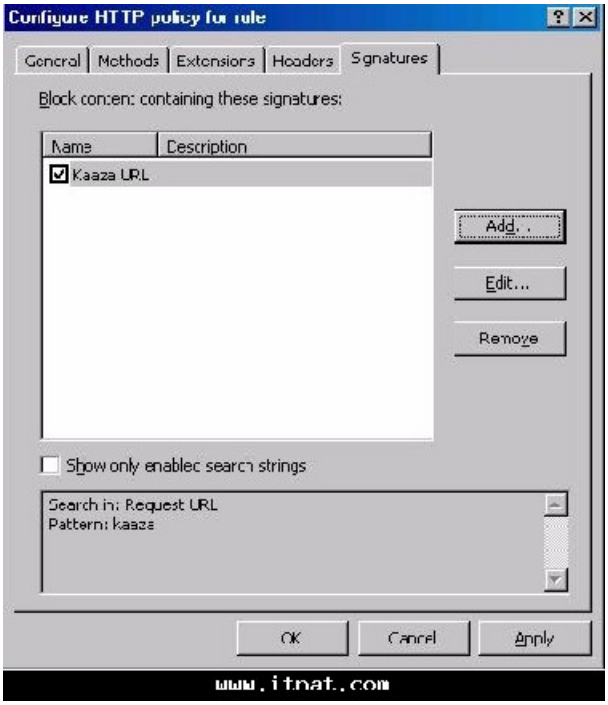
باستخدام سياسة ال HTTP الخاصه بالايزا يمكنك نظريا منع الوصول الى مواقع النت، على سبيل المثال تريد ام تمنع الوصول الى مواقع الانترنت التي تحتوي رابط تحميل برنامج مثل Kaaza كون معظم الملفات المحمله عن طريقه تكون مصابه بالفايروسات وغير مطابقه لقوانين حقوق الطبع.
في الخطوات التاليه سنقوم باعداد سياسة HTTP لمجموعة المدراء والمستخدمين التي تعاملنا معها سابقا لمنع الوصول الى المواقع التي تحتوي اسم. Kaaza
الى الخطوات
1-افتح كونسول ادارة الايزا ثم اذهب الى سياسة الفايروول
2-اضغط باليمين على Administrator Internet Access ثم اضغط علىConfigure HTTP



3-في مربع حوار اعداد سياسة HTTP اضغط على لسانSignatures
4-في لسان Signatures اضغط على اضافه
5-في مربع حوار التواقيع ادخل اسم اسم التوقيع Kaaza URL ثم في قائمه البحث اختار Request URL وادخل الاسم Kaaza في مربع نص التوقيع واضغط اوكي.



6-اضغط تطبيق ثم اوكي



-7الان كرر الخطوات السابقه لقاعدهLimited Access Users

-8اضغط تطبيق واوكي لحفظ الاعدادت الجديده

فحص قواعد الوصول

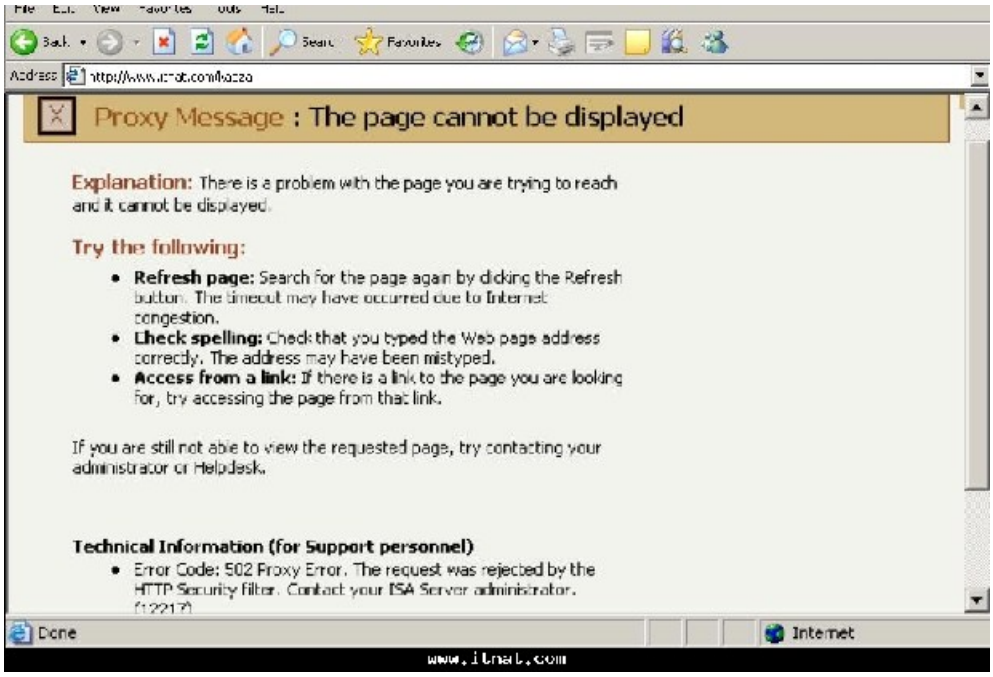
الان بعد ان قمنا بانشاء قواعد وصول مختلفه سنقوم بفحصها كالتالي:

-1افتح كونسول ادارة الايزا اذهب الى سياسات الفايروول ولاحظ قواعد الاتصال في لسان التفاصيل

-2اذهب الى جهاز عميل وادخل باسم مستخدمUser2 ، افتح المتصفح واذهب الى موقع مايكروسوفت.

-3الان ادخل اي موقع اخر لترى رساله ان الموقع لم يتم العثور عليه .
-4الان جرب موقع www.msn.com سترى ان الموقع فتح لكن بعض العناصر الصوريه مفقوده بسبب انها تقع خارج نطاق

-5الان جرب ان تدخل عنوان كالتالي www.itnat.com/kaaza سيعطيك المتصفح رساله خطأ ان الصفحه تم منعها.



-6الان اعمل تسجيل خروج وادخل بحساب Administrator
وجرب الدخول على المواقع اعلاه.

هكذا نكون انهينا هذا الدرس وفيه تعلمنا تقريبا كل شيئ عن سياسات الوصول مع الاخذ بعين الاعتبار ان الطريقه هي نفسها ويبقى عليك كمدير شبكه ان تعرف ما هي البروتوكولات والمواقع التي تريد التعامل معها.

الدرس التاسع
تفعيل خدمة الكاش Cache

-تفعيل خدمة الكاشCaching

تتوفر خدمة الكاش في الايزا السيرفر لتقويه اداء الانترنت واستخدام الباندويدث بشكل اكثر فعاليه. الكاش يعمل على المبدأ التالي، عندما يقوم اي مستخدم بطلب موقع ما فان الايزا يقوم بتخزين الصور والنص والمعلومات الاخرى على الشبكه المحليه، عندما يقوم مستخدم اخر بطلب نفس الموقع فان الايزا يقوم بتوفير جميع العناصر المطابقه من الشبكه المحليه بشكل اسرع من طلبها مره اخرى من الانترنت، يتوقع من الكاش توفير لحد 30-60% من الباندويدث وهذا يعني توفير ايضا على صعيد المال ومصاريف الانترنت.

في البيئه المعقده والكبيره يمكن اعداد الايزا ليقوم بعمل كاش للصفحات المتوقع تحميلها قبل طلبها ايضا للحصول على اعلى قدر من التوفير والسرعه.
الايزا يستخدم ذاكرة الجهاز المنصب عليه للكاش ويفضل تحديد 10% منها اذا كانت 1 جيجا.

خدمات الايزا التي تستخدم الكاش

يستخدم الكاش في الايزا 2004 البروكسي بالاضافه الى الفايروول لتحسين الاداء في عملية التصفح، مبدأ عمل الكاش يعتمد على فحص اذا كان العنصر المطلوب موجود على كاش الايزا المحلي، اذا كان العنصر حالي ومطلوب فان البروكسي يبعث العنصر الى المستخدم من الكاش، اذا كان العنصر غير موجود في الكاش فان البروكسي يطلبها من السيرفر المناسب من الانترنت ويمررها الى المستخدم.

انواع الكاش في الايزا

Forward Caching

هذا النوع يحدث عندما يقوم مستخدم بطلب لمحتوى من الانترنت على شكل HTTP HTTPS FTP ، يمر الطلب في الايزا عندها يقوم الايزا باسترجاع المجتوى من الانترنت ويضع المحتوى في الكاش ويعيد نسخه منه الى المستخدم الذي طلبه من البدايه.

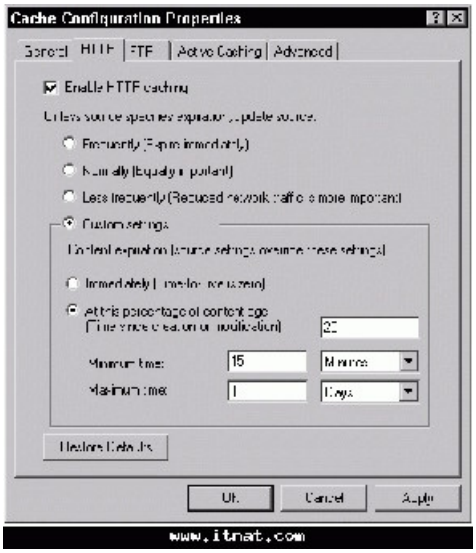
Reverse Caching

يحدث هذا النوع عندما يقوم مستخدم على الانترنت بطلب محتوى موجود على الشبكه الداخليه.

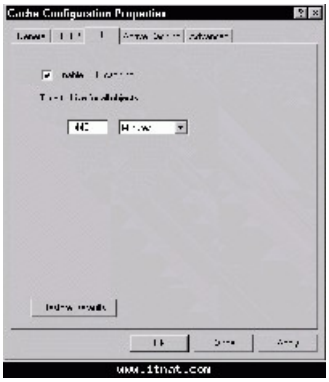
اعداد سياسة الكاش

لا تعتبر جميع مواد الانترنت قابله لان تستعمل في الكاش، والايزا معد مسبقا على ان لا يقوم بادخال صفحات معينه الى الكاش اعتمادا على بيانات رأس الصفحه Headers هذه البيانات لا يتم ادخالها الى الكاش لانها ببساطه لا تعمل بالشكل المطلوب بالكاش، القائمه التاليه تبين رؤوس الصفحات التي يقراها الأيزا ليقرر عدم ادخال الصفحات الى الكاش:
-تحكم الكاش No Cache :امر بسيط يخبر نظام الكاش بعدم ادخال الصفحه الى الكاش
-تحكم الكاش Private :بيانات خاصه لا يجب ادخالها الى الكاش

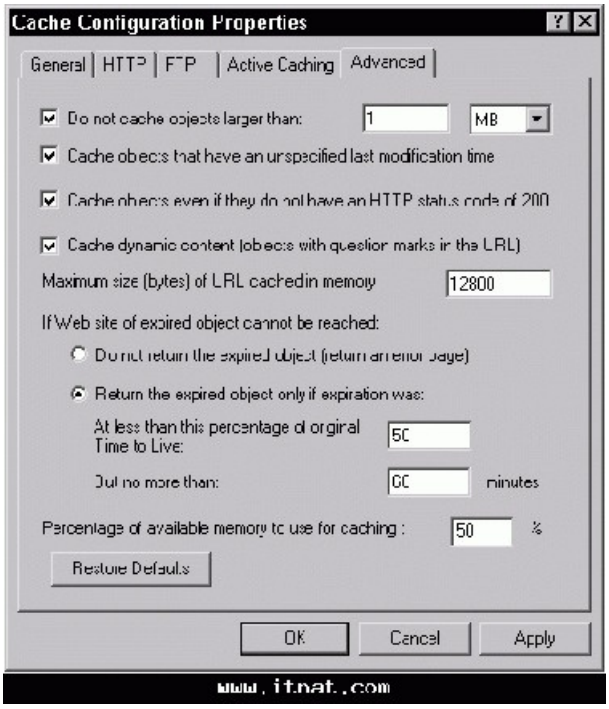
pragme: No Cache -تكون عادة بيانات معالج لا يجب ادخالها في الكاش
www-authenticate -مطلوب التاكيد
set-cookie -صفحة تستخدم كوكي من متصفح المستخدم للتعرف عليه
-طلب لتاكيد الهيدر
-طلب لتاكيد الهيدر – تحكم الكاش : لا تخزين
حتى تتمكن من اعداد سياسة فعالة للكاش عليك اولا الوصول الى خصائص اعدادات الكاش في اداة ادارة الايزا:
-في كونسول ادارة الايزا مدد العقد ثم اذهب الى cache configuration
-اضغط باليمين ثم اختار خصائص
-ستظهر نافذه كالتالي، تلاحظ فيها وجود السنه سنبدأ بلسان HTTP حيث تجد فيه اعدادت تمكنك من ادخال عناصر HTTP الى الكاش.



-اضغط على علامة تفعيل كاش ال HTTP
-اختار خيار Custom settings وثم حدد الفتره التي تريد ان تبقى عناصر ال HTTPفي الكاش، طبعا كلما زادت الفتره قل الضغط على الباندويدث.
-اللسان التالي هو لسانFTP حيث يمكنك من تحديد سياسه الكاش بالنسبه لبروتوكول FTP وفيه ترى ان الكاش مفعل على 1440 دقيقه (24 ساعه)



-اللسان التالي Active Caching في هذا الخيار تستطيع ان تجعل الايزا يقوم بالبحث مسبقا عن العناصر المطلوبه بكثره وادخالها الى الكاش حتى قبل طلبها مما يوفر سرعه عاليه للمستخدمين.
اللسان الاخير هو لسان Advanced ، في هذا اللسان تحدد امرين رئيسين، الاول اعداد ماهية العناصر التي يتم ادخالها الى الكاش والثاني كيف يقوم الايزا بتحديد الذاكرة المتوفره للكاش.



نرى في اللسان الكثير من الخيارات، لكن المهم اول اول مربع وهو يحدد حجم العناصر التي تريد ادخالها الى الكاش وهذا يفيد في عدم تضييع الكاش على عناصر الفيديو والصورة الكبيرة الحجم.
المربع الثاني يحدد للكاش ان يدخل عناصر لا تمللك تاريخ تعديل
الخيار التالي يجعل الايزا يدخل صفحات الى الكاش بدون ان تكون حالتها 200، الحاله 200 في بروتوكول HTTPتعني ان الصفحه تم تحميلها تماما.
الخيار التالي يتيح ادخال عناصر HTTP ديناميكيه الى الكاش مثل نتائج البحث.
الخيار التالي لتحديد الحجم لكل عنوان مخزن في الذاكره واي عنوان اكبر من المحدد لن يتم ادخاله الى الكاش وهذا يساعد في تنظيم ادارة ذاكرة الايزا سيرفر.
ايضا يمكنك استخدام النسبه في الخيار الاخير لتحديد حجم الذاكره المستخدمه.

هكذا تعرفنا على وظيفة مهمه من وظائف الايزا سيرفر وهي خدمة الكاش حيث تمكنك من تخزين الملفات على السيرفر المحلي لتوفيرها الى المستخدمين بشكل اسرع وتوفير اكبر قدر من الباندويدث.

الدرس العاشر
السماح لإتصالات الـ Vpn من خلال الآيزا سيرفر

السماح لإتصالات الـ VPN من خلال الآيزا سيرفر

من مميزات الحائط الناري الخاص بالايزا 2004 انه يمكن ان يجهز كسيرفر شبكه وهميه خاصهVPN ، سيرفرات VPN التقليديه تسمح المستخدمين بالتحكم الكامل بالشبكه التي يتصلون بها، الايزا من جهة اخرى يسمح لمدير الشبكه بتحديد البروتوكولات التي يمكن للمستخدمين الاتصال بها.

تفعيل سيرفرVPN

تلقائيا يكون سيرفر ال VPNغير مفعل على الايزا، لذلك الخطوة الاولى هي تفعيل السيرفر واعداد محتويات

1-افتح كونسول ادارة الايزا ثم مدد اسم السيرفر وتوجه على عقدهVirtual Private Networks (VPN)

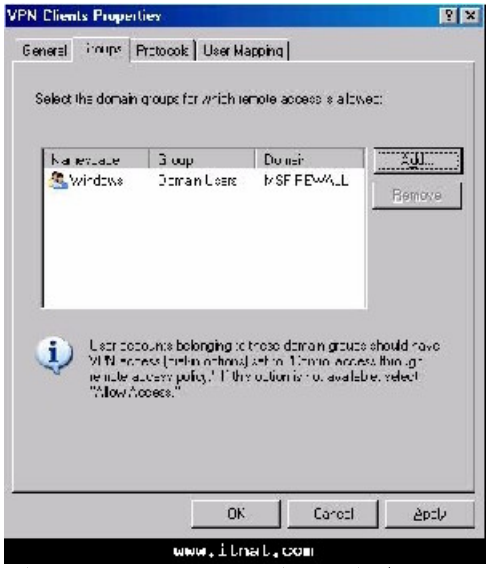
2-الان اضغط على لسان المهمات يمين الشاشه ثم اختارEnable VPN Client Access

3-اضغط تطبيق لحفظ الاعدادات
4-اضغط اوكي
5-اضغط علىConfigure VPN Client Access
6-في لسان General غير قيمة Maximum number of VPN clients allowed من 5 الى 10

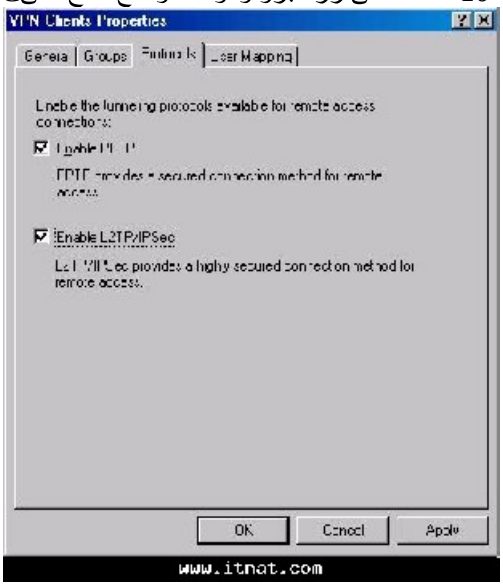
-7اضغط على لسان المجموعات واضغط على زر اضافه

-8في مربع حوار اختيار المجموعات اضغط على زر الموقع، ثم اختار msfirewall.org واضغط اوكي

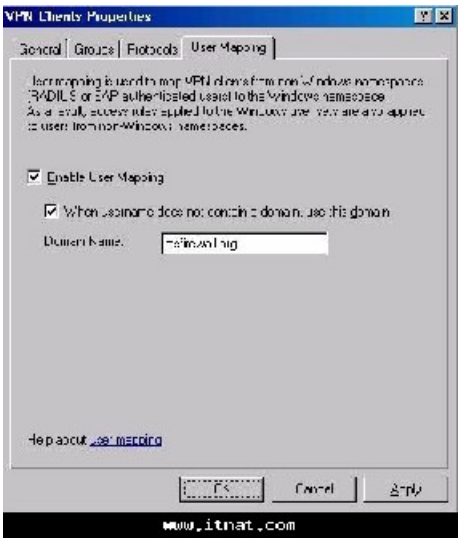
-9في مربع حوار اختيار المجموعات اختار Domain Users واضغط على زر Check Names حيث يحدد اسم المجموعه عند العثور عليه في الاكتيف دايركتوري. اضغط اوكي.



-10اضغط على زر البروتوكولات وضع صح علىL2TP/IPSEC



-11اضغط على لسان User Mapping ثم ضع صح على خيار .Enable User Mapping ضع صح على خيار When user name does not contain a domain, use this domain واضغط على msfirewall.orgفي مجموعة النطاقات.



12-اضغط على تطبيق واوكي لتظهر رساله بان الايزا يجب ان يعاد تشغيله لتاخذ الاعدادات مجراها.

انشاء قاعدة وصول للسماح بمستخدمي ال VPN بالوصول الى الشبكه الداخليه

حتى هذه اللحظه فان مستخدمي ال VPNيمكنهم الاتصال بسيرفر ال VPNلكنهم لا يستطيعون الوصول الى الي مصدر من مصادر الشبكه.لذلك علينا انشاء قاعدة وصول للسماح لهم بالوصول الى الشبكه الداخليه

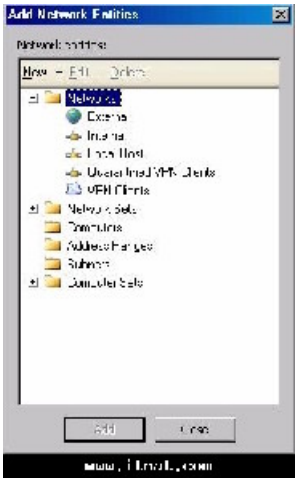
1-افتح كونسول ادارة الايزا واذهب الى عقده Firewall Policy اضغط باليمين ثم جديد ثم قاعدة وصول.

2-في صفحة الترحيب ادخل اسم القاعدة الجديده مثلا VPN Client to Internet واضغط التالي

3-في صفحة اجراء الوصول اضغط على سماح ثم التالي

4-في صفحة البروتوكولات اختر جميع البروتوكولات الخارجيه من قائمه This rule applies to ثم التالي

5-في صفحة مصادر القاعدة اضغط على اضافه ثم اضافه كيان شبكه، في مجلد الشبكات اختر VPN Clients واضغط اغلاق.



-6اضغط التالي

-7في صفحة Access Rule Destination اختر اضافه ثم كيانات ثم اختار الشبكات بعدها اختار الشبكه الداخليه واضغط اغلاق
-8في صفحة المستخدمين اضغط التالي
-9اضغط انهاء
-10اضغط تطبيق ثم اوكي

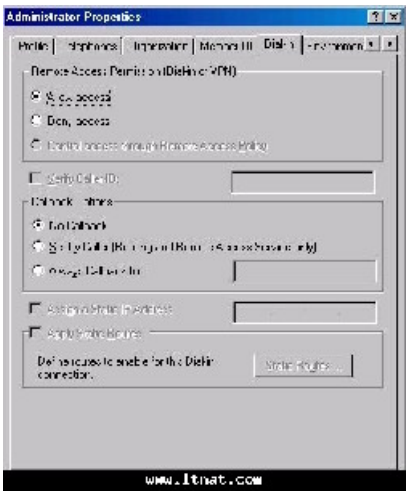
تفعيل الوصول عن طريق الاتصال Dial-Up لحساب الادمن

يعتمد الوصول عن طريق الدايل اب على طبيعة البيئه المحليه للاكتيف دايركتوري حيث انه يكون مفعل في بيئه اكتيف دايركتوري Native والعكس صحيح، لذلك الافضل هو التاكد من تفعيل الخدمه على كل مستخدم كالتالي

-1اذهب الى Domain Controller ثم اضغط على ابدا Administrative Tools ثم Active Directory Users and Computers

-2في كونسول ادارة المستخدمين على الاكتيف دايركتوري اذهب الى عقدة المستخدمين ثم اضغط مرتين على مجموعة الAdministrator

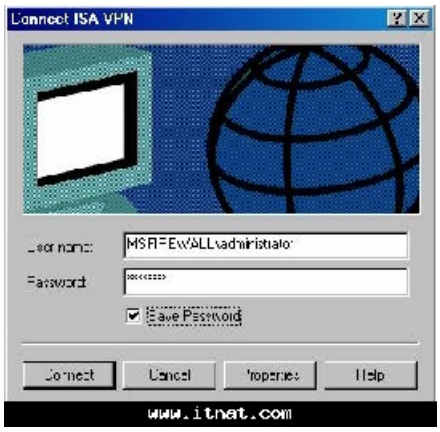
-3اضغط على لسان الاتصال Dial-Up سترى في المربع الاول السماح بالاتصال VPN اختر السماح ثم تطبيق ثم اوكي



-4اغلق كونسول ادارة الاكتيف دايركتوري

فحص اتصال ال VPN

قم باجراء الخطوات التاليه لفحص سيرفر ال VPNالتابع للايزا سيرفر
-1سنفترض ان المستخدم الخارجي يعمل على ويندوز 2000 ، نذهب الى My Network Places ونختار خصائصها بالضغط عليها باليمين
-2ستظهر نافذة وصلات الشبكه والاتصال اختر انشاء وصله جديده
-3اضغط التالي في الرساله الترحيبيه
-4في صفحة نوع الاتصال اختر اتصال الى شبكه خاصه عبر الانترنت
-5في صفحة العنوان ادخل 192.168.1.70 واضغط التالي
-6في صفحة توفر الاتصال اجعلها متوفره لجميع المستخدمين
-7لا تقم باجراء اي تغييرات على مشاركة الانترنت ثم اضغط التالي
-8ادخل اسم الوصله الان مثلا ISAVPN واضغط انهاء
-9الان سيظهر مربع الاتصال ادخل كالتالي



المستخدم MSFIREWALL\Administrator :
كلمة السر
حيث ان MSFIREWALL هو اسم سيرفر الايزا
و Administrator هو اسم المستخدم الذي تريد الاتصال عن طريقه
-10الان سيقوم الجهاز بالاتصال با VPN Serverويستخدم نظام تشفير MPPE 128 لحماية الاتصال على الانترنت.

-11لاظهار المجلدات المشتركه على متحكم الدومين اكتب التالي في سطر الاوامر

\\Exchange2003be وهو اسم متحكم الدومين في حالتنا.
هكذا نكون انشانا اتصال VPN ناجح بين جهازين على الانترنت حيث يستطيعان تبادل الملفات والمعلومات بامن وسريه كامله.

شرح برنامج GFI WebMonitor لإدارة مستخدمي الإنترنت من خلال الآيزا سيرفر

ملخص :نواجه صعوبة ومن خلال برنامج الايزا سيرفر في إدارة المستخدمين في الشبكة، حيث ومن خلال هذا البرنامج يمكننا الحد من تحميل جميع انواع الملفات او جزء منها ، كما ويمتاز البرنامج بفحص الملف من الفايروسات قبل تحميله على الجهاز، ويمكنك ومن خلاله أيضاً عمل مجموعات، يمتاز البرنامج بقوة أدائه وتقاريره الرائعة، حيث يمكنك معرفة جميع التحركات التي حدثت من طلب مواقع وكمية سحب بيانات، والملفت للنظر في هذا البرنامج بأنه يمكنك رؤية ما يتم تحميله بنفس الوقت وكذلك فصل عملية التحميل بالضغط على إيقاف، كل جهاز على حدى .

صفحة البرنامج:
http://www.gfi.com/webmon/

الجوائز التي حصل عليها:
http://www.gfi.com/webmon/webmonreviews.htm

شرح له باللغة الإنجليزية:
حمل ملفPDF

شرح باللغة العربية:

سهولة مراقبة الانترنت
مع خاصية GFI WebMonitor مدراء الشبكة باستطاعتهم الان الوصول الى الاجهزة التي تعمل على الانترنت ومشاهده المواقع التي يقوموا بفتحها ومساحة الباندويث التي يقومو بسحبها وهو يقوم ايضا باضافة برامج مكافحة الفايروسات على الشبكة وتصل الي 50 مستفيد.

التحكم بالشبكة وحمايتها من الفايروسات عن طريق برنامج.BitDefender
باتحاد GFI WebMonitor و BitDefender انتي فايروس يقوم بحماية الشبكة 100% من الفيروسات وكما تمتلك ICSA حقوق هذا البرنامج وقد نال برنامج BitDefender درجة 100% في مكافحة الفيروسات لسنة 2006 حسب تقييم الشركات وجائزة تكنولوجيا المعلومات الاوروبيه سنة 2002. وبهذا تكون عملية الحماية على الشبكة بشكل كبير جدا.

حماية الشبكة من ملفات (التجسس، والتروجان ... الخ) عن طريق خيارات برنامج الحماية.Kaspersky
الان تستطيع تحقيق المزيد من الامن للشبكة ومسح الفايروسات مع برنامج مكافحة الفيروسات Kaspersky، برنامج كاسبر سكاي يستطيع ان يكشف ملفات التروجان التي باستطاعتها سرقة كلمة الدخول وكلمة المرور للشخص ويقوم بمسحها تلقائيا.

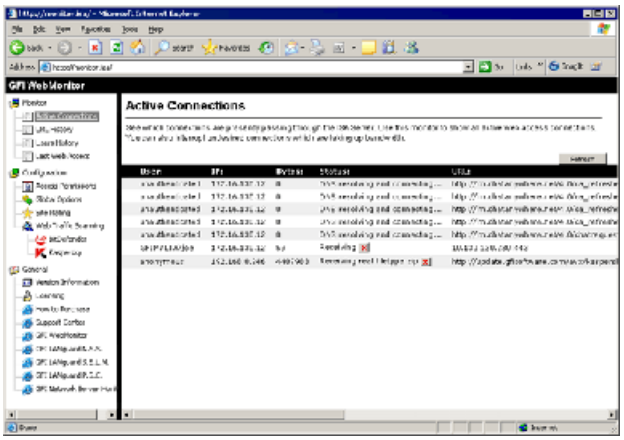
حماية الاشخاص من فتح المواقع غير المرغوب فيها والقيام بحبث امن.
يسمح لك GFI WebMonitor باغلاق صفحات الانترنت الغير مراد فتحها وهو يتيح لك الوقت الكافي لعمل ترشيح كامل لصفحات الغير مراد فتحها من غير ان تاخذ وقت طويل في كتابة اسماء الصفحات. ويعطيك GFI WebMonitoمعلومات كافية عن المواقع التي تحتوي على صفحات للراشدين فقط.
اغلاق الداونلود او الاتصال في وقت محدد.
الان مع خاصية تحديد وقت استخدام الانترنت باستطاعة الادمن على الشبكة ايقاف التصفح او الغاء التحميل وبامكانه ايضا تحديد من يرغب في اغلاق الانترنت او التحميل على الاشخاص المعنين.

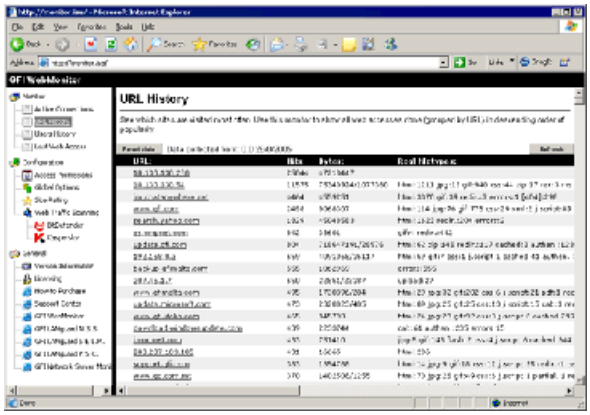
حماية من تهديدات مخترقي المواقع.
من غير القدرة على اصحاب المواقع حماية مواقعهم بشكل تام من تهديد اختراق الموقع وبتركيب ادوات GFI بامكانك حماية موقع من هذه التهديدات ومنع الوصول الى المواقع الاباحية التي تكثر مثل هذه الملفات عليها.
سهولة اغلاق صفحات الويب مع خاصية ISA blocking واغلاء الوصل الى عناون الصفحة المراد اغلاقها.

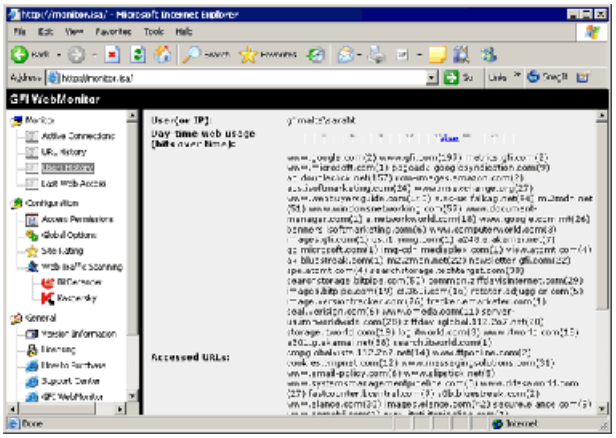
فحص واغلاق تطبيقات التحميل المخفية.
هناك بعض تطبيقات التحميل تعمل تلقائيا عند فتح صفحة معينة باستخدام HTTP وهذا يقلل من امكانية الادمن السيطره على الشبكة لانه يمكن نقل الفايروسات وملفات التجسس من دون معرفة اسم المستخدم و GFI WebMonitorيسمح لك بمراقبة المستخدمين والملفات المتداولة.

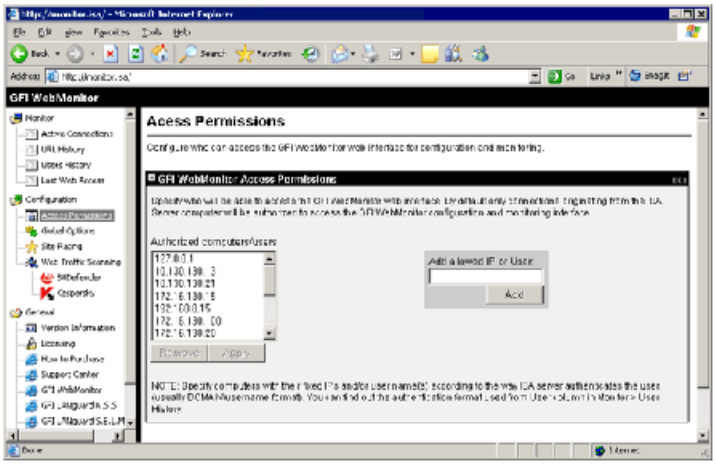
مراقبة الاعدادت وشاشة العرض.
GFI WebMonitorيسمح لك باختيار الاشخاص الذي تريد ان تكون لهم صلاحيات كاملة او غير كاملة.
ويمكن ان تحدد هذه الصلاحيات من خلال الاي بي لكل شخص او اسم المستخد او الدومين.

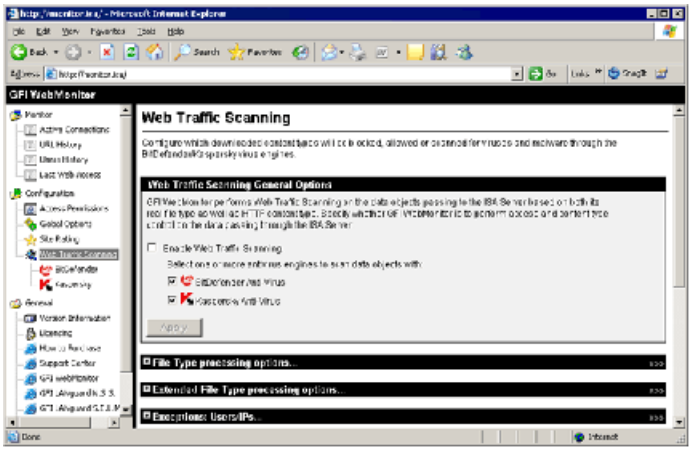
بعض الصور للبرنامج:

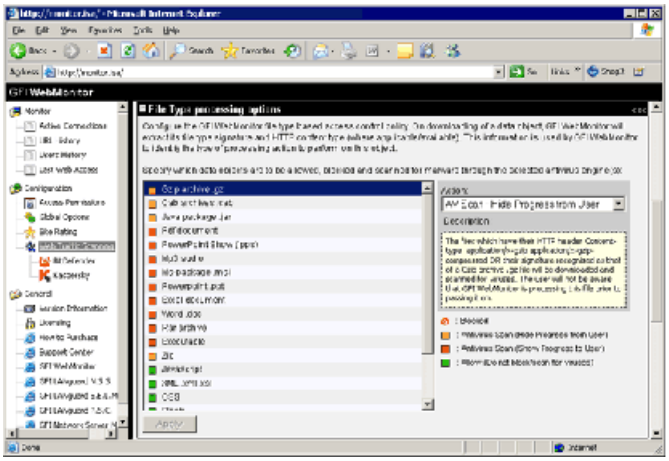


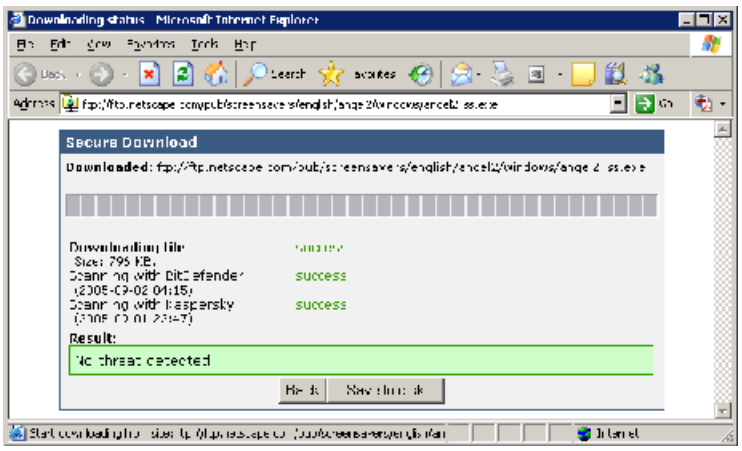

GFI WebMonitor
URL History


GFI WebMonitor
Accessed URLs:


GFI WebMonitor
Acess Permissions
GFI WebMonitor Access Permissions







يمكنك شراء البرنامج من خلال شبكة الجيل الجديد للتكنولوجيا

شرح برنامج Bandwidth Splitter للتحكم بالسرعة من خلال الآيزا سيرفر

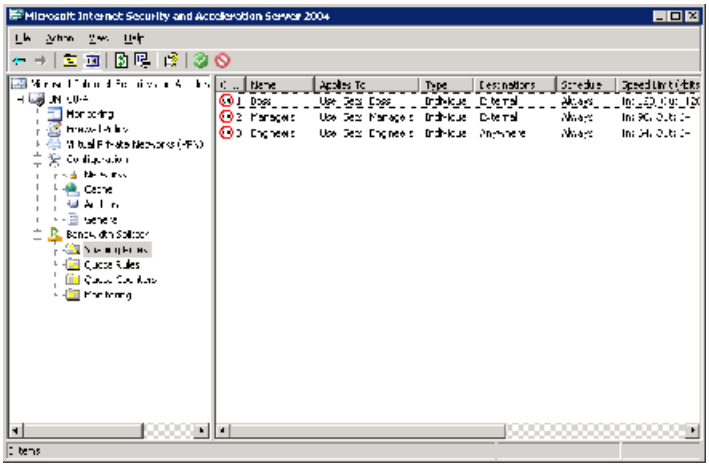
ملخص :يعتبر البرنامج من أقوى وأولى البرامج التي تتحكم بالباندويدث من خلال الآيزا سيرفر ، حيث يمكنك تحديد السرعة لكل مستخدم بطريقة سهلة ،، بالإضافة إلى إمكانية مشاهدة عمليات التحميل التي تتم بنفس اللحظة ،، ننصح به لقوة تحمله وسرعة أدائه وسهولة تنصيبه .

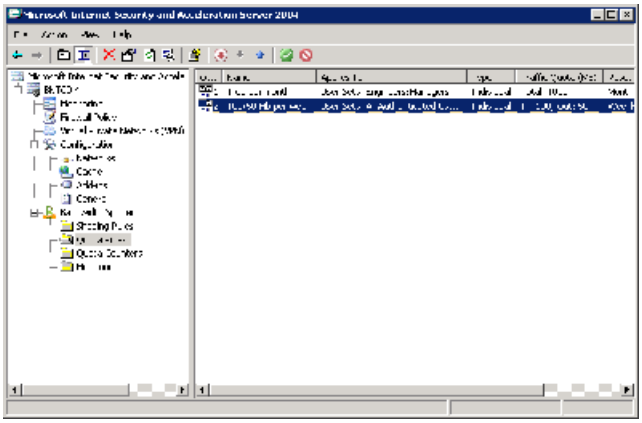
اسم البرنامجBandwidth Splitter :
يعمل على جميع نسخ آيزا سيرفر 2000 ، 2004، 2006

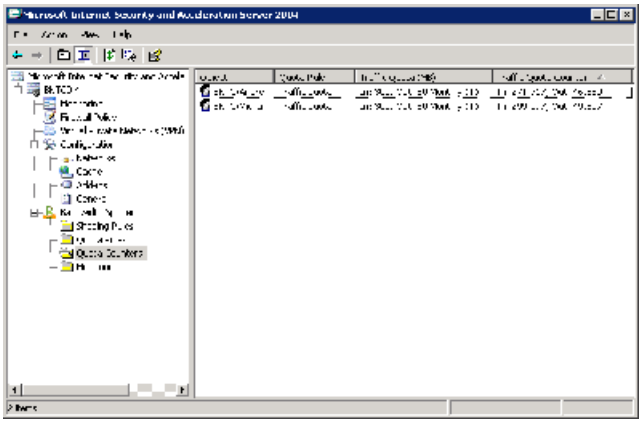
البرنامج مجاني لعشرة أشخاص فقط
موقع البرنامج :http://www.bsplitter.com/
رابط تحميله :
Bandwidth Splitter v.1.13 for ISA Server 2000
Bandwidth Splitter v.1.05 for ISA Server 2004/2006

نحن الوكلاء الوحيدون بالشرق الأوسط لهذا البرنامج، لمزيد من المعلومات اضغط هنا
http://www.bsplitter.com/resellers.aspx

صور من البرنامج :







الخطوات.

- بعد الانتهاء من تثبيت الايزا سيرفر وادارة المفاتيح بشكل تام (إمكانية التحك بها.(
- قم بتحديد الترافيك لكل من HTTP, HTTPS و) FTP لتحديد البروكسي للمستخديمن) و TCP/UDP)لمستخدمي FWC و(SNAT ، نسخة ISA 2004/2006 قادرة على ادارة الترافيك الخاص TCP/UDP لل DMZ servers باستخدام ISA Server ا في NAT او.router
- قم بتحديد الترافيك المنتشر على السيرفر.
- قم بعمل اعدادت للباندويث للمستخدمين (عن طريق حسابات(AD ، والاستضافة) عن طريق الاي بي)، وقم بطلب عنوان السيرفر.
- حتى قناة التوزيع داخل مجموعات المستخدمين (في حال عرض الباندويدث المخصصة لمجموعة المستخدمين.(
- حتى توزيع الباندويدث للاتصالات النشطة لكل مستخدم.
- من الممكن وضع حدود للسرعة وحصص منفصله للمستقبل و/ أو للخارج او الاثنين معا.
- تحديد عدد من الوصلات لاحد المستخدمين و المضيفين.
- في بعض أنواع الصفحات، يمكنك تحديد سرعة الداون لود لمستوى معين بحيث تكون اعلى اول اقل من الاخرين لكي لا يصبح العمل والاتصال بطئ.
- من الممكن تحديد مقدار داون لود لا نهائي لكاش صفحات الويب.
- تحديد الترافيك للمستخدمين، المضيفين، مجموعات المستخدمين او مجموعات المضيفين، يومي، اسبوعي، شهري او من دون تحديد وقت مع الاحتمال اعادة توزيع التنرافيك تلقائيا الى الفترة المقبلة.
- من الممكن عدم اخذ كاش الويب من داخل الترافيك الخاص بالمستخدمين.
- من الممكن عدم اخذ الترافيك او لجهات معددة او في وقت معين من داخل التارفيك الخاص بالمستخدمين.
- مراقبة الوقت الحقيقي للمستخدمين والمضيفين يسمح للانترنت من خلال ISA Server مع تفاصيل المعلومات عن كل الاتصالات، ويشمل على استخدان الباندويث برسم رسوم بيانية تحدد الكمية المسحوبة.
- الشفافيه للمستخدمين : انك لا تحتاج الى أي تركيب برامج للمستخدم على الحاسوب.
- احتمالية استخدام المستخدمين الوقت الحقيقي الخاصة برصد ومتابعة كميو البااندويدث في الوقت الحقيقي.
- دعم ما يصل الى الاف المستخدمين للعمل معا.
- اداء عالي المستوى مع خفض الود على الكمبيوتر.
- مجانا لعدد مستخدمين يصل الى 10.

خدمات الاتصالات.

Bandwidth Splitterيتم بناءه على ISA Server باستخدام الويب ونظام فلترة التطبيقات للتحكم

بالترافيك من خلال ISA Server.
Bandwidth Splitter يدعم بقوة:
•بروكسيات الويب الخارجة HTTP, HTTPS and FTP.
•اتصلات Firewall للمستخدمين كل اتصالات TCP/UDP.
•اتصلات SecureNAT للمستخدمين لكل اتصالات TCP/UDP.
•اتصالات published servers.
•اتصالات من خلال انشاء فلترة للتطبيقات.
•تقرير انزال محتوى الاتصالات.
•نسخة ISA 2004/2006 تدعم فقط: كل اتصالات routed TCP/UDP من خلال ISA Server من DMZ servers.

Bandwidth Splitter لا يدعم:
•المستوى الادنى. TCP/UDP
•فقط ل: الاتصال بين شبكة Local Host واي شبكة اخرى. ISA 2004/2006
•في : ISA 2000 تدعم Routed IP التي تشل كل البيانات المنتقلة من خلال DMZ

لطلب البرنامج من خلالنا اضغط هنا

انتهى الكتاب آملين من الله ان نوفق به
ولا تنسونا من حسن الدعاء

مع تحيات شبكة الجيل الجديد للتكنولوجيا
www.itnat.com